por los Derechos Civiles

Acuerdo sobre comercio electrónico del MERCOSUR: Desafíos y oportunidades

Julio 2022

Investigación y Redacción:
Celia Lerman, Gabriela Szlak y Lucía Suyai Mendiberri

Revisión y Edición:
Asociación por los Derechos Civiles (ADC) y Alianza del Comercio Digital (en inglés, Digital Trade Alliance)

Diagramación y Diseño:
Biri Biri

Con el apoyo de Public Citizen

Resumen Ejecutivo

El 29 de abril de 2021, en la sede central del Mercosur los representantes de Argentina, Brasil, Paraguay y Uruguay celebraron el Acuerdo sobre Comercio Electrónico del Mercosur (el "Acuerdo").

En el presente trabajo analizamos su impacto en la protección de datos personales en los Estados parte y en el desarrollo del comercio electrónico en la región. Para ello, evaluamos primero el contexto en el cual surge el Acuerdo, tanto respecto del crecimiento exponencial del comercio electrónico local, especialmente tras los efectos de la pandemia de Covid-19, como de otros acuerdos, documentos e iniciativas internacionales en el marco del Mercosur. Seguidamente, analizamos en detalle sus artículos y destacamos diversos ejemplos de su futura aplicación.

Además, nos detenemos en el marco regulatorio local de los Estados Parte, analizando para cada territorio el impacto del Acuerdo en los diversos aspectos principales en materia de protección de datos: los estándares internacionales, incluyendo principios generales tales como el previo consentimiento, finalidad, calidad, seguridad, responsabilidad, entre otros; las medidas de seguridad; las transferencias internacionales de datos y las comunicaciones comerciales directas no solicitadas. También comparamos al Acuerdo con otros instrumentos internacionales en materia de datos personales y economía digital, incluyendo otros acuerdos comerciales regionales como el Acuerdo de Asociación de Economía Digital (DEPA, por su sigla en inglés), el Acuerdo Transpacífico de Cooperación Económica (CPTPP, por su sigla en inglés), y los Acuerdos de Libre Comercio entre Argentina y Chile, y Uruguay y Chile, cuyas similitudes permiten concluir que sus textos sirvieron de fuente directa.

Para terminar, brindamos tres conclusiones principales: (1) Argentina, Paraguay y Uruguay deberán adaptar su legislación local de protección de datos personales para cumplir con el texto del Acuerdo; (2) la similitud del texto del Acuerdo con otros convenios internacionales de comercio muestra su valor para que el Mercosur retome negociaciones internacionales con la Unión

Europea y con los países del CPTPP; y [3] la promoción del comercio electrónico y de la co-regulación en el Mercosur puede ser positiva para la protección de los datos personales, la privacidad y los derechos humanos en la región. Con estas conclusiones, dilucidamos las oportunidades y desafíos que el Acuerdo presenta para la protección de datos y el desarrollo del comercio electrónico en el Mercosur.

Contenido

1. Introducción

La Asociación por los Derechos Civiles (ADC) es una organización de sociedad civil que desde 1995 trabaja en la promoción y defensa de los derechos fundamentales en Argentina y América Latina poniendo especial atención a personas y grupos sociales en situación de vulnerabilidad. Durante la última década, la innovación tecnológica trajo riesgos únicos para el acceso y el ejercicio de los más variados derechos y, en consecuencia, ADC ha procurado integrar a su labor una perspectiva digital.

Desde 2020 ADC forma parte de la Alianza del Comercio Digital, en inglés Digital Trade Alliance (DTA), una coalición global que promueve una agenda pro-usuario/consumidor en las discusiones sobre comercio digital. En el marco de la DTA y con el apoyo de Public Citizen, ADC encomendó a las reconocidas abogadas, Celia Lerman, Gabriela Szlak y Lucía Suyai Mendiberri esta investigación. Luego de un arduo trabajo realizado entre fines de 2021 y principios de 2022, las autoras y el equipo de ADC han arribado conjuntamente a las consideraciones expuestas a continuación.

El 29 de abril de 2021, en la sede central del Mercosur en Montevideo, Uruguay, representantes de Argentina, Brasil, Paraguay y Uruguay celebraron el Acuerdo sobre Comercio Electrónico del Mercosur (el "Acuerdo"). [(1)]

Éste se compone de 16 artículos, a través de los que se propone establecer los presupuestos mínimos de un marco jurídico común para el comercio electrónico en las jurisdicciones de los Estados parte, con la finalidad de aprovechar el potencial económico y las oportunidades proporcionadas por dicha actividad. A tales efectos, en materia de comercio electrónico, se incluyen disposiciones para la protección al consumidor/a en línea [(2)] y la ubicación de instalaciones informáticas [(3)]. También se introducen principios sobre el acceso y uso de internet para el comercio electrónico y sobre la cooperación entre los Estados [(4)].

Asimismo, el Acuerdo incluye el deber de los Estados parte de garantizar la regulación del derecho de los usuarios y las usuarias a la protección de sus

datos personales [(4)]. En esta materia se observan disposiciones específicas sobre la transferencia transfronteriza de información por medios electrónicos y las comunicaciones comerciales directas no solicitadas.

El objetivo principal de este trabajo es analizar el impacto del Acuerdo en la protección de datos personales en los países del Mercosur y en el desarrollo del comercio electrónico en la región. A tal fin, en primer lugar, evaluamos el contexto en el cual surge, centrándonos en el crecimiento exponencial del comercio electrónico en la región, especialmente tras los efectos de la pandemia Covid-19. Así como en otros acuerdos, documentos e iniciativas internacionales en el marco del Mercosur: el Mercosur Digital, el Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital, la Resolución Mercosur 37/19 sobre Defensa del Consumidor y Protección al Consumidor en el Comercio Electrónico, y el posible Acuerdo Mercosur - Unión Europea.

En segundo lugar, analizamos en detalle los artículos que encontramos más relevantes del Acuerdo, evaluando su texto concreto en cada caso y destacando diversos ejemplos de su futura aplicación. En tercer lugar, nos detenemos en el marco regulatorio local de los Estados parte, evaluando para cada territorio el impacto del Acuerdo en aspectos centrales en materia de protección de datos: los estándares internacionales, incluyendo principios generales tales como el previo consentimiento, finalidad, calidad, seguridad, responsabilidad, entre otros.

En cuarto lugar, comparamos al Acuerdo con otros instrumentos internacionales en materia de datos personales y economía digital: revisamos el Convenio N°108 del Consejo de Europa y los Estándares de Protección de Datos de los Estados Iberoamericanos; así como los acuerdos de Asociación de Economía Digital, en inglés Digital Economy Partnership Agreement (DEPA) celebrado en 2020 entre Singapur, Chile y Nueva Zelanda; el Acuerdo Transpacífico de Cooperación Económica, en inglés Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) celebrado en 2018, y los Acuerdos de Libre Comercio entre Argentina y Chile y Uruguay y Chile, cuyas similitudes con el Acuerdo del Mercosur permiten concluir que sus textos sirvieron de fuente directa para éste.

Para finalizar, brindamos tres conclusiones principales: (1) Argentina, Paraguay y Uruguay deberán adaptar su legislación local para cumplir con el texto del Acuerdo; (2) la similitud del texto del Acuerdo con otros convenios internacionales de comercio muestra su valor para que el Mercosur retome negociaciones internacionales con la Unión Europea y con los países del CPTPP; y (3) la promoción del comercio electrónico y de sistemas de co-regulación en el Mercosur puede ser positiva para la protección de los datos personales, la privacidad y los derechos humanos en la región. Con estas conclusiones, dilucidamos las oportunidades y desafíos que el Acuerdo presenta para la protección de datos y el desarrollo del comercio electrónico en el Mercosur.

2. Antecedentes

2.1. El comercio electrónico en América Latina. Efectos de la pandemia de Covid-19[5]

"Si bien 2020 pasará a la historia como uno de los años más tumultuosos para la industria del retail en América Latina, también será recordado como el año en que la región se convirtió en el mercado del comercio electrónico de retail de más rápido crecimiento en el mundo". [6]

En un mundo en constante innovación, la evolución de la utilización de las Tecnologías de la Información y las Comunicaciones (TIC) en materia económica, y en especial para desarrollar el comercio electrónico, va dando lugar a nuevas técnicas de comercialización de productos y servicios. Asimismo, trae aparejada nuevos modelos de negocios, formas de organización social y empresarial, hábitos de consumo, y no menos importante, nuevas estructuras regulatorias que, en ausencia de avances significativos a nivel multilateral, se verifican tanto a nivel local, como regional. Así, según S. Herreros (CEPAL, 2019) los acuerdos comerciales preferenciales que contienen disposiciones sobre comercio electrónico son "muy diversos en su amplitud y profundidad, lo que refleja las distintas visiones de los principales actores de la economía digital sobre cómo se debe regular dicho comercio" [7]. En este sentido, las regulaciones a nivel regional, en este caso a nivel del Mercosur, se proponen armonizar las normativas locales y de esa forma fomentar e impulsar estos desarrollos con miras a aprovechar el potencial económico y las oportunidades que entrañan para los miembros del bloque.

En los últimos años previos a la pandemia, tanto la oferta (empresas que ofrecen bienes y servicios a través de internet) como la demanda (consumidores/as que eligen internet como canal de compra) se fueron poco a poco sofisticando en la región del Mercosur. La carrera por la conquista del comercio electrónico en los países del bloque, en particular en el sector retail, continuó año tras año con tasas de aumento y mejoras constantes, lo que dio

lugar al incremento en la cantidad y la calidad de los productos ofrecidos en línea. De este modo muchísimas pequeñas y medianas empresas (pymes) [8] comenzaron a promocionar sus productos y servicios en internet [9].

En aquel tiempo también, se puede verificar un aumento constante en el número de usuarios y usuarias con disposición a realizar compras en línea, quienes como consumidores/as fueron aprendiendo y adoptando las nuevas tecnologías disponibles [10]. Esta evolución se apoyó en diversos factores como las políticas nacionales y regionales en materia de inclusión digital, la innovación impulsada por el sector empresarial, la fuerte penetración en la región de la telefonía móvil con acceso a internet, el aumento y profesionalización de la oferta de productos y servicios, la mejora continua en la seguridad y confianza de las transacciones digitales, entre otros [11]. Sin embargo, según la opinión experta, antes de la pandemia el comercio electrónico minorista en la región de América Latina todavía se encontraba rezagado en su adopción y más aún en el contexto transfronterizo [12]. Según S. Herreros, "en el caso de América Latina y el Caribe, su participación estimada en las ventas mundiales del comercio electrónico transfronterizo es muy inferior a su participación en las exportaciones mundiales de bienes, que durante la presente década ha oscilado alrededor del 5,5%." (2019) [13]

Ahora bien, en 2020 se vio un fuerte aumento de todos los indicadores del comercio electrónico en el mundo, siendo América Latina una de las regiones protagonistas de este crecimiento global de la actividad [14]. Según eMarketers, los efectos de la pandemia llevaron a la región a transformarse en la industria minorista de comercio electrónico que más rápido creció en el mundo [15]. Este récord de crecimiento implica que 38 millones de latinoamericanos/as fueron compradores/as digitales por primera vez en 2020 [16].

Según se indica, los motivos de este crecimiento pueden encontrarse en los efectos de la pandemia y las medidas tomadas por los gobiernos para su prevención y contención, como el cierre de las tiendas físicas. Si bien esta desafortunada circunstancia provocó una catástrofe para muchas empresas de la región en cuanto a las ventas tradicionales, desde el punto de vista del

comercio electrónico minorista, significó una increíble oportunidad que fue ciertamente aprovechada. De esta forma, observamos en todos los países de la región un crecimiento mucho más alto de lo esperado por los pronósticos previos a la pandemia.

En este sentido, en Brasil (la economía más fuerte del bloque) comprar en línea se transformó en la "nueva normalidad" durante 2021[(17)]. Esta tendencia se replicó en el caso de Argentina al observarse que, según el informe de la Cámara Argentina de Comercio Electrónico, las ventas totales del comercio electrónico crecieron un 124% en 2020 [(18)].

Algunos analistas creen que el impulso que ha tenido el comercio electrónico a partir de 2020 no sólo llegó para quedarse, sino que seguirá en permanente aumento y que no existirán retrocesos aún considerando la cotidianidad de la post-pandemia. Lo cierto es que los indicadores de crecimiento del comercio electrónico en la región latinoamericana en 2020 y el primer semestre de 2021, son cuanto menos, impactantes.

En virtud de lo expuesto se puede afirmar que el comercio electrónico ha escalado y se ha potenciado, y que el avance -tanto para la oferta como para la demanda- continuará abriendo nuevas oportunidades. Sin embargo, existen aún muchos desafíos para la región. Dentro de cada uno de los países del bloque, por ejemplo, existen retos pendientes en materia de inclusión digital y financiera respecto de las personas consumidoras (demanda), así como desafíos de capacitación y profesionalización de los recursos humanos, respecto de las pymes (oferta). Asimismo, la región cuenta con desafíos pendientes en materia de comercio electrónico transfronterizo, tanto intrabloque como de los países del bloque para con otros países.

En este punto es importante mencionar que el comercio electrónico transfronterizo de bienes tangibles (productos) que no tenía números elevados en la región antes de la pandemia, ha tendido a la baja en 2020 tanto en Brasil como en Argentina, las dos economías más grandes del bloque [(19)]. Desde la perspectiva del consumidor/a, en Argentina se vieron muy limitados para

acceder al comercio electrónico transfronterizo, mientras que en Brasil tuvieron un crecimiento leve con un 10% en 2019 que subió a 14.2% en 2020 [(19)]. Entre los aspectos que suelen afectar al consumidor/a de la región a la hora de comprar en línea de forma transfronteriza, diversos reportes de comercio electrónico han identificado: las limitaciones, el encarecimiento y la complejidad de los aspectos y costos impositivo/aduaneros; la percepción de inseguridad, y falta de confianza y de diversidad en los medios de pago disponibles.

Ahora bien, desde la perspectiva de la oferta aparecen algunas barreras de acceso importantes también para las empresas que desean exportar bienes y servicios a través del comercio electrónico a consumidores/as transfronterizos/as. Si bien una plataforma de venta online o incluso una página de una red social pueden servir como "vidriera al mundo", al querer concertar una transacción que cruza fronteras la oferta, en especial las pymes, se encuentra con obstáculos de diferente índole. Por ejemplo, en Argentina, si bien el 51% de las empresas manifestó en 2020 su interés en vender al exterior, sólo el 7% lo logró y dentro de ese porcentaje el 58% se trató de venta de pasajes y turismo, lo que no implica resolver cuestiones de logística ni aduaneras de productos atravesando fronteras. Las razones identificadas por las empresas como obstáculos para vender a nivel transfronterizo fueron, por orden de relevancia, cuestiones de logística, impositivas, falta de información y temas de facturación [(20)].

Es por ello que entendemos que el Acuerdo resulta oportuno tanto para las empresas como para los y las consumidoras en el Mercosur, aunque existen múltiples factores que exceden el presente análisis, y que afectan el desarrollo del comercio electrónico a nivel transfronterizo. El Acuerdo se propone establecer un marco jurídico que armonice la regulación en los Estados parte a fin de potenciar el comercio electrónico intrabloque y sus oportunidades para todos los actores, garantizando reglas comunes y abordando, en particular, los derechos de las personas consumidoras y usuarias, dentro de los que encontramos la cuestión de la privacidad y de la protección de sus datos personales.

Vinculado a esto último, no podemos dejar de mencionar el valor estratégico de los datos (no solo los de carácter personal) como activo transable e

intangible. En este sentido "...los flujos transfronterizos de datos han tenido un crecimiento exponencial en lo que va transcurrido de este siglo" [(21)]. En efecto, se ha dicho que "el comercio electrónico transfronterizo, al involucrar a agentes ubicados en distintas jurisdicciones, está sujeto a un mayor grado de incertidumbre que las transacciones locales. En este contexto, los factores institucionales son cruciales para generar la necesaria confianza entre las personas y las empresas. Por ejemplo, contar con leyes que garanticen un grado adecuado de privacidad de los datos personales y que protejan a los consumidores en línea contra prácticas fraudulentas es esencial para que las personas se atrevan a participar en este tipo de intercambio." [(22)]

Por último, el Acuerdo responde a una tendencia del Mercosur de unificar criterios y regulación en materia de comercio electrónico intrabloque. En esta línea, también se inserta la Resolución 37/2019 de Defensa del Consumidor. Protección al Consumidor en el Comercio Electrónico, que fue incorporada recientemente en los ordenamientos locales de cada país [(23)]; el Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital [(24)]; entre otros que se referirán a continuación.

2.2. Acuerdos, documentos e iniciativas internacionales relevantes del Mercosur

2.2.1. Mercosur Digital

En el 2017 se creó el Grupo Agenda Digital del Mercosur ("GAD") con el objetivo de "promover el desarrollo de un Mercosur Digital". Este grupo tiene entre sus principales iniciativas la armonización de las políticas nacionales de protección de datos personales, el desarrollo de un mecanismo integrado online para solución de controversias relacionadas con operaciones de e-commerce y proyectos conjuntos para el desarrollo del comercio electrónico transfronterizo [(25)].

El GAD es responsable del impulso de muchas de las normativas que se refieren en este documento como, por ejemplo, el Acuerdo sobre Comercio Electrónico

del Mercosur en sí, el de Reconocimiento Mutuo de Certificados de Firma Digital y otros.

2.2.2. Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital

El Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital resulta de gran importancia a los efectos del comercio electrónico entre las jurisdicciones de los Estados parte, ya que, como su nombre lo indica, tiene por finalidad reconocer la validez de la firma digital emitida en cada uno de ellos [(26)]. Mediante este documento la firma digital emitida conforme a los procedimientos de cada país y a través de los prestadores de servicios de certificación acreditados por cada Estado parte tiene el mismo valor que la firma manuscrita.

El texto establece ciertos lineamientos generales que deben cumplir las firmas digitales en cuestión, tales como: responder a estándares internacionales, contener datos que permitan identificar inequívocamente al titular y al prestador de servicios de certificación, ser susceptible de verificación respecto de su estado de revocación, ser emitidas por un prestador de servicios de certificación acreditado bajo el sistema nacional de acreditación y control de infraestructuras de claves públicas. Además, el acuerdo define ciertos lineamientos de aspectos operativos para la evaluación y armonización de las prácticas de certificación.

De todos modos, es importante tener en cuenta que, la Firma Digital no se encuentra lo suficientemente difundida, ni entre las empresas que ofrecen productos y servicios a través del comercio electrónico, ni entre consumidores/as y empresas que compran o venden por internet, en ninguno de los países del bloque. En consecuencia, entendemos que este Acuerdo, por sí sólo no podrá garantizar el uso a nivel intrabloque de esta herramienta, sino que deberá ser fomentada y difundida por cada uno de los Estados parte.

En lo que respecta puntualmente a la protección de datos personales, el ordenamiento se limita a referir que los prestadores de servicios de certificación deberán cumplir con la legislación en la materia vigente en el Estado, donde se haya obtenido su licencia o acreditación.

2.2.3. Resolución Mercosur 37/19. Defensa del Consumidor. Protección al Consumidor en el Comercio Electrónico

La Resolución Mercosur 37/19 [(27)] establece lineamientos generales a fin de armonizar la legislación de los Estados parte en materia de defensa del consumidor y consumidora y fue oportunamente incorporada al ordenamiento de cada país [(28)]. Esta normativa incluye, por ejemplo, obligaciones específicas de proveer información al/la consumidor/a durante el proceso de transacción e identificación del proveedor. Además, el documento obliga a los proveedores a poner a disposición los términos y condiciones de contratación, y copias de estos documentos. Sin embargo, en este documento no existen disposiciones específicas en materia de protección de datos personales.

2.2.4. Posible Acuerdo Mercosur - Unión Europea

En el 2019 circuló el texto de un posible acuerdo de comercio entre Mercosur y la Unión Europea que incluía ciertas disposiciones en materia de comercio electrónico ("Posible Acuerdo Mercosur Unión Europea") [(29)]. Al respecto, se establece entre sus objetivos detectar las posibilidades y promover el comercio electrónico entre las partes. Además, de aprobarse el acuerdo, se regularía entre otras cuestiones: (i) la neutralidad tecnológica del comercio electrónico [(30)]; (ii) la facultad de terminación del contrato por medios electrónicos [(31)]; (iii) el reconocimiento de la validez de la firma electrónica [(32)]; (iv) las comunicaciones de marketing no consentidas [(33)]; y (v) la protección de los consumidores; entre otros puntos.

En este documento, en materia de comercio electrónico y protección de datos personales, únicamente se advierte la prohibición de enviar comunicaciones de marketing no consentidas, lo que en definitiva recepta el principio del

consentimiento como base legal para el tratamiento de datos personales. Sin embargo, seguidamente se reconoce la facultad de enviar este tipo de comunicaciones a consumidores/as con los que se tenga una relación previa y sólo sobre productos o servicios similares a los que hubieran contratado [(34)]. Tal como se observará más adelante, este mismo texto es adoptado por el Acuerdo sobre Comercio Electrónico del Mercosur, objeto de este documento.

2.2.5. Acuerdos de Libre Comercio entre Argentina y Chile y Uruguay y Chile

En 2016, Chile y Uruguay negociaron y celebraron un Acuerdo de Libre Comercio (ALC) que regula un conjunto de materias y disciplinas comerciales de diversa índole, incluyendo el comercio electrónico [(35)]. Este acuerdo entró en vigor en 2018. Asimismo, Argentina y Chile celebraron, también en 2016, un acuerdo comercial para continuar avanzando en la integración bilateral que entró en vigor en 2019 [(36)]. El texto de ambos acuerdos respecto de las provisiones de comercio electrónico (y entre ellas, la protección de datos personales) es muy similar, casi una réplica del texto del entonces Acuerdo de Asociación Transpacífico, en inglés Trans-Pacific Partnership (TPP) luego recogido por el CPTPP.

3. El Acuerdo sobre Comercio Electrónico del Mercosur

Este Acuerdo, eje central del análisis del presente trabajo, tiene por finalidad 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.

Regular la materia del comercio electrónico comprende también la protección de los datos personales y otros temas relacionados que entendemos que traen aparejadas implicancias para esta temática, tal como se analizará en detalle a continuación.

3.1. Artículo 1. Definiciones

Dentro de las definiciones que trae el Acuerdo en lo que hace a la protección de datos personales, podemos encontrar que se define al "dato personal" como cualquier información sobre una persona física identificada o identificable. Esta definición sigue las tendencias internacionales en la materia, aunque no necesariamente se adecúa a las legislaciones actuales de los países del bloque, como sucede en el caso de Argentina, Uruguay y Paraguay. En lo que respecta a estos países, la definición de "dato personal" bajo la normativa vigente también abarca a cualquier información relativa a personas jurídicas y no solamente a personas físicas.

Otra de las definiciones que trae el artículo, que por lo general se refiere a una temática que es abordada por las normativas de datos personales de cada uno de los países, es la de "comunicaciones comerciales directas no solicitadas". Tal como se refirió en apartados anteriores, en el ámbito del comercio electrónico la protección de datos personales en muchos casos se traduce en la prohibición (con algunas excepciones) de enviar comunicaciones de marketing no consentidas, receptando el principio del consentimiento para el tratamiento de datos personales. En este sentido, el Acuerdo define a estas comunicaciones como "un mensaje electrónico que se envía con fines comerciales o publicitarios a la dirección electrónica de una persona sin el consentimiento del destinatario, o contra el rechazo explícito del destinatario" [(37)]. Esta cuestión es luego retomada por el Acuerdo en su artículo 10, comentado más abajo.

3.2. Artículo 2. Ámbito de aplicación y disposiciones generales

Bajo su artículo segundo, el Acuerdo establece que, al considerar el potencial del comercio electrónico como instrumento de desarrollo social y económico, las partes reconocen la importancia de algunas cuestiones particulares. Destacamos que este texto es virtualmente idéntico al texto del artículo 11.2 del Acuerdo de Libre Comercio entre Argentina y Chile, que entró en vigor en 2019, así como del artículo 8.2 del Acuerdo de Libre Comercio entre Uruguay y

Chile, que entró en vigor en 2018 [38].

Resaltamos los siguientes puntos en relación con los temas que nos ocupan en este análisis:

Punto 5. b: Alentar la autorregulación en el sector privado para promover la confianza y la seguridad jurídica en el comercio electrónico, teniendo en cuenta los intereses y los derechos de los usuarios a través de iniciativas tales como las directrices, modelos de contratos, códigos de conducta y sellos de confianza;

Punto 5. e: Facilitar el acceso al comercio electrónico por las micro, pequeñas y medianas empresas y;

Punto 5. f: Garantizar la seguridad de los usuarios del comercio electrónico, así como su derecho a la protección de datos personales. A su vez, en la nota señalada se agrega que este derecho refiere a que la recolección, así como el almacenamiento de datos, deberán realizarse siguiendo principios generales en la materia, como el previo consentimiento, finalidad, calidad, seguridad, y responsabilidad, entre otros [39].

Este último punto será abordado a lo largo del presente trabajo. Ahora bien, entendemos los puntos 2.5.(b) y 2.5.(e), referidos a la autorregulación en el sector privado para promover la confianza y la seguridad jurídica en el comercio electrónico, y a facilitar el acceso al comercio electrónico por las pymes, como intrínsecamente relacionados y también -de una forma indirecta- vinculados con los aspectos de la protección de datos personales. Esta redacción debe verse como un supuesto de co-regulación conforme se desarrollará en el punto 3.11 de este apartado, bajo el cual los Estados sientan las bases mínimas de regulación y los privados complementan el marco normativo.

3.3. Artículo 5. Protección al consumidor en línea

Bajo este artículo las partes reconocen la importancia de proteger a los y las consumidoras de prácticas fraudulentas y engañosas cuando participen en el comercio electrónico. En este orden, se establece la obligación de las partes de ajustar la normativa en la materia a lo establecido por el MERCOSUR.

Cabe mencionar que la protección de los y las consumidoras establecida bajo este artículo respecto de las prácticas fraudulentas y engañosas también sería aplicable al tratamiento de los temas de seguridad y protección de datos personales que se lleve a cabo en el marco del comercio electrónico.

Entendemos que los Estados han preferido no extenderse en la regulación sobre este punto en tanto sus normativas internas resultan dispares, tal como se releva a lo largo de este trabajo, y no todos otorgan los mismos niveles de protección o cuentan con una legislación detallada sobre el tema. No obstante, incluir compromisos de este tipo sienta las bases para el desarrollo de la normativa interna en la materia. Eso es lo que sucede con las diferentes resoluciones dictadas por el MERCOSUR al respecto, que luego son incorporadas por los países a nivel local. Un ejemplo lo constituye la Resolución 37/2019 de Defensa del Consumidor. Protección al Consumidor en el Comercio Electrónico ya citada, la que fue incorporada recientemente en los ordenamientos locales de cada país [(40)].

3.4. Artículo 6. Protección de datos personales

La protección de los datos personales se regula específicamente bajo el artículo 6 del Acuerdo. Resulta interesante que, a modo de declaración, su inciso 1 refiere a la importancia que tiene la protección de los datos personales para la confianza en el comercio electrónico. Lo anterior se encuentra efectivamente alineado con las buenas prácticas en la materia.

El inciso 2 del artículo establece que las partes deberán adoptar y mantener leyes, regulaciones o medidas administrativas para la protección de la información personal. Al respecto, se indica que deberán tomarse en consideración los estándares internacionales que existen en la materia.

El inciso 3 dispone que cada parte deberá hacer esfuerzos para que su marco legal doméstico en materia de protección de datos personales sea aplicado de forma no discriminatoria. En relación con esto último, entendemos que este tipo de disposiciones responden al espíritu de armonización normativa que

pretende el Acuerdo, y a la tendencia de los acuerdos de comercio que suelen incorporar disposiciones como ésta, a fin de garantizar que la regulación no sirva como una barrera o impedimento al comercio.

En línea con los objetivos de armonización del Acuerdo, en los siguientes incisos 4 y 5 se incluyen disposiciones específicas tales como la obligación de los Estados parte de publicar información sobre la protección de los datos personales que se reconoce a los usuarios y las usuarias del comercio electrónico en cuanto a los derechos de acceso, rectificación y supresión, y de las obligaciones para las empresas. Aún más, bajo el inciso 8 del artículo 6 se establece que las partes deberán arbitrar medios para establecer medidas comunes para la protección de los datos personales y su libre circulación en el Mercosur. En igual línea, la cooperación en el desarrollo de regulación común se advierte a partir del compromiso expreso de los Estados parte de intercambiar información y experiencias en cuanto a su legislación de protección de la información personal.

La obligación de implementar medidas de seguridad en el tratamiento de datos personales se inserta en el inciso 6 de este artículo, al establecer que las partes deberán fomentar la utilización de mecanismos de seguridad, disociación o anonimización en el caso que los datos personales sean brindados a terceros [(41)].

A fin de velar por un nivel adecuado de protección de datos personales en las jurisdicciones, el inciso 7 establece que las partes deben garantizar tal nivel de protección a través de una norma general, regulación específica o acuerdos mutuos. En lo que refiere al sector privado, se reconoce la posibilidad de implementar contratos o mecanismos de autorregulación a fin de cumplir con tal requisito de nivel de protección. Al respecto cabe destacar que, como ya fue referido anteriormente, el Acuerdo se inserta en una práctica de co-regulación exigiendo, por un lado, la implementación de leyes y una activa participación normativa del Estado y, por el otro, reconociendo la posibilidad de implementar contratos o mecanismos de autorregulación, incluida también en el Art. 2.5.(b) [(42)].

La autorregulación responde a la tendencia normativa en materia de protección de datos personales que reconoce la capacidad de los privados para establecer un marco normativo que cumpla con los estándares de protección de los titulares de los datos requerido por la ley. Es decir que la autorregulación es aceptable en este contexto, sólo dentro de los parámetros que establece la ley y para los puntos que ella específicamente habilita por lo que se entiende como un esquema de co-regulación. Por ejemplo, Argentina prevé que los niveles adecuados de protección pueden provenir de cláusulas contractuales y de sistemas de autorregulación, estableciéndose el estándar que tales mecanismos deben cumplir mediante resoluciones específicas emitidas por la autoridad de control [(43)].

3.5. Artículo 7. Transferencia transfronteriza de información por medios electrónicos

Al expedirse sobre la transferencia internacional de datos personales, el Acuerdo libra a los Estados parte para que éstos establezcan los requisitos regulatorios de conformidad con lo establecido bajo el Artículo 6.

A su vez, se establece en el inciso 2 que deberá permitirse la transferencia cuando ello se requiera para la realización de actividades comerciales (la que estará sujeta a lo dispuesto por el artículo 6 sobre los requisitos de niveles adecuados de protección). Con relación a este punto, el Acuerdo expresamente refiere a que esto no podría significar un impedimento para que un Estado adopte o mantenga medidas para alcanzar un objetivo legítimo de política pública [(44)]. No obstante, esta discrecionalidad no podrá traducirse en una restricción al comercio.

Por último, cabe mencionar que las disposiciones de transferencia transfronteriza de datos personales dispuestas bajo el Acuerdo no resultan aplicables a los servicios financieros [(45)]. Entendemos que esta excepción tiene relación con que los datos referidos a esta industria suelen estar regulados de forma específica por la legislación y por ello el Acuerdo, dirigido a la industria del comercio electrónico, no los abarca. Destacamos también que, como

veremos en detalle, el Acuerdo se inspira en los textos del CPTPP y del DEPA, que también brindan regulación específica para los servicios financieros [(46)].

En relación con la excepción respecto de servicios financieros, cabe mencionar que será interpretada de forma restrictiva en los países que ya tienen una regulación específica en materia de transferencia internacional de datos. Por ejemplo, Argentina y Uruguay incluyen expresamente esta excepción en lo que respecta al régimen aplicable a las transferencias internacionales de datos sólo respecto de "transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;" [(47)].

Por su parte, Brasil no incorpora la excepción de los servicios financieros por lo que no sería operativa respecto de este país. En el caso de Paraguay, tal como se detalla más adelante, no existe al momento una reglamentación respecto del régimen aplicable a las transferencias internacionales de datos. No obstante ello, cabe puntualizar que se han presentado diferentes proyectos de ley en busca de adecuar la normativa en la materia. Estos no incluyen una excepción de este tipo por lo que no sería operativa, como sucede en el caso de Brasil [(48)].

3.6. Artículo 8. Ubicación de las instalaciones informáticas

El artículo 8 dispone que las partes podrían imponer requisitos regulatorios relativos al uso de instalaciones informáticas, incluyendo aquellos necesarios para asegurar la seguridad y confidencialidad de las comunicaciones [(49)].

En esta misma sección se refiere al principio de territorialidad, prohibiendo expresamente incorporar obligaciones de establecimiento de instalaciones informáticas en el territorio como condición para la realización de negocios allí [(50)]. Sin embargo, se prevé que esto no podría entenderse como un impedimento para que cada parte alcance objetivos legítimos de políticas públicas, otorgando margen a los Estados para incorporar este tipo de restricciones [(51)]. Así, si bien aparece una prohibición expresa, se estaría permitiendo establecer requisitos de territorialidad a los Estados parte siempre que se basen en razones legítimas de políticas públicas. Por otro

lado, para evitar interpretaciones amplias, el mismo artículo dispone que las mencionadas razones no deberán aplicarse de forma que constituyan un medio de discriminación arbitrario o injustificable, o una restricción encubierta al comercio [(52)]. En este sentido, entendemos que el Acuerdo buscaría de esta forma evitar la discriminación arbitraria para con los proveedores tecnológicos, así como barreras al desarrollo, en coincidencia con la mirada de algunos/as autores/as [(53)].

A su vez, al introducir el artículo de territorialidad se establece expresamente que usar o ubicar fuera del territorio las instalaciones informáticas donde se alojan datos personales será considerado una transferencia internacional. También se aclara nuevamente en este apartado que estas disposiciones no serán aplicables a los servicios financieros.

Por último, existen incipientes discusiones en algunos de los países del MERCOSUR respecto de la conveniencia o inconveniencia de establecer normas de localización. Por ejemplo, en Argentina en el 2017 se presentó un proyecto de ley de "Soberanía de Datos" que tenía por fin prescribir que ciertos datos generados por el sector público sean almacenados exclusivamente en territorio argentino. Su objetivo era mantener la soberanía sobre dichos datos y poder garantizar su accesibilidad y resguardo en cumplimiento con las regulaciones vigentes del Estado Nacional [(54)]. Estas discusiones explican posiblemente por qué el Acuerdo toma la postura de establecer una prohibición expresa para seguidamente, permitir el establecimiento de requisitos de territorialidad a los Estados parte, siempre que se basen en razones legítimas de políticas públicas y con las demás aclaraciones que buscan impedir barreras al desarrollo del comercio electrónico.

3.7. Artículo 9. Principios sobre el acceso y uso de Internet para el comercio electrónico

A través de este artículo los Estados parte reconocen los beneficios de la capacidad de los consumidores y las consumidoras de acceder y usar los servicios y aplicaciones de su elección. Si bien no se recoge expresamente

el concepto en este documento, estas condiciones parecen receptar cierto principio de neutralidad de la red que excede el objeto de este trabajo.

En definitiva, esta declaración refuerza el compromiso de los Estados parte para garantizar las condiciones necesarias para el desarrollo del comercio a través de internet.

3.8. Artículo 10. Comunicaciones directas no solicitadas

En línea con la normativa aplicable en materia de comunicaciones no solicitadas, bajo la sección 10 del Acuerdo se establece que se deberá procurar proteger de manera efectiva a los usuarios y las usuarias finales contra las comunicaciones comerciales directas no solicitadas [(55)]. El texto es idéntico al que se adopta en el posible acuerdo entre el Mercosur y la Unión Europea en su Artículo 48, y es por ello que entendemos que debe interpretarse a la luz de los preceptos europeos en este ámbito [(56)].

El Artículo 10 establece que debe (i) asegurarse que no se envíen comunicaciones comerciales no solicitadas a los consumidores que no hayan dado su consentimiento [(57)] y (ii) asegurarse que las comunicaciones directas no solicitadas sean identificables como tales, revelen quién las envía y contengan información necesaria para que los usuarios puedan ejercer su derecho de solicitar de manera gratuita al remitente el cese en el envío de este tipo de comunicaciones. En relación con este último punto, se busca que se informe acerca del derecho de retiro o bloqueo también denominado derecho de oposición, conocido en la esfera del marketing como la posibilidad de ejercer el opt-out de una determinada lista de distribución de envío de correos electrónicos.

En lo que respecta al consentimiento para las comunicaciones no solicitadas, se indica que el mismo será definido conforme a las leyes y disposiciones de cada Estado parte y que se permitirá que se envíen este tipo de comunicaciones si se hubiera recolectado el dato en el marco de la venta de un producto o servicio, siempre que sea sobre los propios productos o servicios similares. Nos

parece relevante en relación con este punto traer algunas reflexiones relativas a la realidad de las prácticas de la región en materia de comunicaciones comerciales directas y de marketing digital en general. En este sentido, por un lado, nos encontramos con que muchas empresas, en especial las pymes, cuyo negocio principal no está asociado a la tecnología, se encuentran lejos de cumplir con las reglas mínimas de protección efectiva de los usuarios y las usuarias contra las comunicaciones comerciales directas no solicitadas.

Las empresas referidas en el párrafo anterior, en muchos casos, suelen enviar comunicaciones comerciales directas a bases de datos de usuarios/as no depuradas, en las que es altamente probable que se desconozca si han brindado su consentimiento o no para recibir tal comunicación. Esto no significa necesariamente que el usuario o la usuaria, no haya brindado su consentimiento, sino que simplemente la empresa no ha seguido procesos adecuados que permitan conocer esta circunstancia respecto de los datos personales en sus bases de datos. Un ejemplo clásico es aquella empresa que toma los datos de sus usuarios/as en locales de venta presencial, a través de un empleado o empleada que ingresa a la base de datos de la empresa, datos personales que son brindados en forma espontánea y oralmente por quienes visitan el local para recibir información o participar de alguna acción de marketing específica.

Otra de las cuestiones que se observan en la práctica de la región es la problemática de que las empresas no cuentan con procesos ni tecnologías uniformes, ni con bases de datos centralizadas. Tampoco cuentan con sistemas que permitan dar de baja datos personales de determinadas bases, en varias bases de datos al mismo tiempo, o que se realice el pedido de retiro o bloqueo en una determinada base pero no en todas a la vez.

Las problemáticas referidas son sólo algunas de las que existen y provocan en los usuarios y las usuarias de la región una percepción de que las empresas les envían comunicaciones directas no solicitadas y de las falencias en el cumplimiento del requerimiento de no seguir recibiendo las comunicaciones comerciales directas.

Sin perjuicio de la problemática introducida en párrafos anteriores, también nos encontramos ante un proceso de desarrollo y profesionalización en la región, en el que las empresas dedicadas específicamente a proveer servicios de email marketing tanto para las pymes como para grandes empresas siguen las tendencias internacionales en la materia. Estas empresas trabajan desde criterios de consentimiento, al que denominan opt-in. Podemos ver un ejemplo de esto en los eventos denominados "eMail Marketing Summit" llevados a cabo en Argentina, por AMDIA (actualmente, DMA Argentina), la Asociación de Marketing Directo e Interactivo de Argentina, junto a las empresas de la industria del email marketing, que ya por el año 2019 incluyó entre sus disertaciones una sección dedicada específicamente a la protección de datos personales [(58)]. Además, la industria del email marketing viene demostrando que las campañas de marketing basadas en el envío de correos electrónicos obtienen mayores resultados y retorno de la inversión cuando la publicidad es recibida por quien está efectivamente interesado en ella. Es decir, las métricas y mejores prácticas se alinean con cuestiones de carácter normativo y la exigencia del consentimiento.

Ahora bien, en lo que refiere a la industria de la publicidad y el marketing digital, se advierte que actualmente se extendieron técnicas para la personalización y automatización en el envío de comunicaciones comerciales, que no dejan de traer aparejados desafíos intrínsecos en materia de protección de datos personales tanto para la región como a nivel global. Estas técnicas permiten conocer los hábitos de consumo y comportamiento de los usuarios y las usuarias por medio del seguimiento de sus actividades en línea y el entrecruzamiento de datos, lo que en combinación con tecnologías de perfilamiento personaliza y automatiza el envío de comunicaciones comerciales. Esto se produce no sólo a través de correo electrónico, sino todo tipo de publicidad que las personas usuarias reciben en diversas plataformas digitales, aplicaciones móviles y sitios web en los que navegan. Las plataformas digitales actuales, tales como, motores de búsqueda, mapas en línea, plataformas de contenidos, juegos, aplicaciones mobile y redes sociales, entre otras, no suelen involucrar transacciones monetarias con consumidores/as (es decir, funcionan de forma "gratuita"). En este sentido, lo que ofrecen es una

especie de intercambio implícito con sus usuarios/as en el que estos "pagan" por los servicios, brindando información y datos personales (no siempre de forma consciente), los que son compartidos en esas plataformas o tomados por éstas por medio de técnicas de seguimiento (trackeo). Luego los datos son tratados por múltiples empresas, por medio de la utilización intensiva de tecnologías tales como machine learning y algoritmos especializados, todo lo cual es finalmente monetizado, no sólo por dichas plataformas sino también por muchas otras empresas, mediante la compraventa de publicidad personalizada en tiempo real, perfilada para cada usuario/a.

En este sentido, atendiendo a las nuevas prácticas y tendencias en la industria de la publicidad y el marketing digital, se puede decir que el avance de la regulación en la región "llega tarde" [(59)]. Mientras tanto, desde la perspectiva de los usuarios y las usuarias, la discusión en materia de publicidad y marketing digital versus privacidad y derechos humanos es mucho más profunda y recién empieza [(60)].

La discusión actual en la materia se asocia a la utilización intensiva de las técnicas mencionadas, que junto con la utilización de big data generan prácticas de publicidad en línea en muchos casos invasivas y no necesariamente consentidas, con profundas implicaciones para los derechos humanos como es la privacidad. Estas cuestiones, afectan al corazón del funcionamiento de la internet comercial como la conocemos hoy, y son una cuenta pendiente en materia de privacidad y derechos humanos a nivel global.

En este sentido, valoramos algunas iniciativas, tanto provenientes de la industria como de la sociedad civil, para tratar esta compleja problemática que requiere abordar la necesidad de apostar por la innovación y el desarrollo de la economía digital; procurar una internet abierta y accesible; y al mismo tiempo mitigar al máximo los riesgos inherentes respecto de derechos humanos como la privacidad. Un ejemplo de estas iniciativas es la denominada MyData que, sin dejar de valorar la importancia que el intercambio y flujo de datos personales conlleva hoy para la economía digital, reúne a emprendedores/as, activistas, académicos/as, corporaciones, agencias públicas y desarrolladores/as con la misión de empoderar a los individuos en el derecho a la autodeterminación

informativa. MyData cuenta con una comunidad que trabaja en pos del uso ético de los datos personales, por medio de una visión alternativa y la difusión de principios técnicos para el tratamiento de datos personales basado en la confianza [(61)].

En línea con lo expuesto, se ha insistido en que ante el advenimiento de nuevas tecnologías resulta clave el reconocimiento de derechos de autodeterminación informativa de los y las titulares y el empoderamiento como el que propone MyData, todo esto junto con la responsabilidad corporativa y la intervención estatal. El trabajo conjunto de privados y los Estados llevaría a establecer un marco en el que estos últimos desempeñan un papel clave en asistir a los individuos en sus derechos y a las compañías en la gestión de la privacidad, equilibrándose la intervención reguladora y la innovación empresarial. En este contexto cobra especial relevancia la co-regulación como se refería en apartados anteriores, que requiera a los privados la implementación de un sistema de co-regulación determinado para obtener un permiso estatal que habilite el tratamiento de datos [(62)].

3.9. Artículo 12. Cooperación

Bajo este artículo las partes expresan su entendimiento sobre la naturaleza global del comercio, en particular del electrónico, y en consecuencia, de la importancia de la cooperación. Así, el documento sólo parece reflejar cierto compromiso de las partes en sentar bases para negociar el desarrollo de la normativa en la materia. En este marco se comprometen, entre otras cuestiones a:

- Trabajar conjuntamente para facilitar el uso del comercio electrónico, generar mejores prácticas, mejorar las oportunidades de las micro y pequeñas empresas [(63)];
- Compartir información y experiencias sobre leyes, regulaciones, programas de esfera del comercio electrónico, incluyendo las relacionadas a la protección de los datos personales, entre otras.
- Posibilitar el intercambio de datos estructurados y estandarizados bajo normas que permitan la interoperabilidad de los sistemas y el acceso oportuno a las transferencias de datos.

3.10. Cumplimiento del Acuerdo y resolución de controversias

El Acuerdo no prevé un sistema específico de resolución de controversias. Es por ello que, ante el incumplimiento de una parte, será aplicable el Sistema de Solución de Controversias del Mercosur, regulado en el "Protocolo de Olivos" (PO)[(64)]. De acuerdo con este sistema, las partes involucradas deben primero procurar resolver la controversia por negociaciones directas (art. 4 PO). Si mediante las negociaciones directas no arribaran a un acuerdo completo, cualquiera de los Estados parte puede iniciar directamente el procedimiento arbitral ad hoc del Mercosur (previsto en el Art. 9 PO y siguientes) o someterla primero a consideración del Grupo Mercado Común (art. 6 PO). Los laudos de los tribunales ad hoc son obligatorios para los Estados parte de la controversia y son revisables por el Tribunal Permanente de Revisión (art. 26 PO). Resulta pertinente destacar que desde la creación del sistema de resolución de controversias en 1998, y con anterioridad a la entrada en vigor del PO, es decir durante la vigencia del Protocolo de Brasilia y su Reglamento (aprobado por Decisión CMC Nº 17/98), se dictaron diez laudos arbitrales. Por otro lado, el sistema de Solución de Controversias también prevé etapas anteriores y paralelas tales como procedimientos de Consultas y de Reclamaciones, regulados por la Directiva CCM Nº 17/99, y por el Anexo del Protocolo de Ouro Preto y la Decisión CMC Nº 18/02, respectivamente. Tales mecanismos son gestionados por la Comisión de Comercio del MERCOSUR (CCM) y el Grupo Mercado Común (GMC) [(65)].

Sin perjuicio de la aplicabilidad del Sistema de Solución de Controversias del Mercosur o de los procedimientos de Consultas y de Reclamaciones paralelos o previos, entendemos que, por la naturaleza del Acuerdo, resulta poco probable que un Estado parte denuncie el incumplimiento de otro a través de dicho sistema. Y si eso sucediera, el Sistema de Solución de Controversias, así como el de Consultas y Reclamaciones, podrían activarse para dirimir las cuestiones planteadas.

3.11. Co-regulación bajo el Acuerdo

A lo largo del texto del Acuerdo existen algunas referencias a la "autorregulación" (como sucede en el artículo 2.f). La autorregulación ha sido objeto de fundadas críticas en cuanto a su eficacia respecto del bien general. Asimismo, su incapacidad para lograr los objetivos pretendidos ha incluso dado lugar a las regulaciones modernas en materia de protección de datos personales en Europa y Estados Unidos [(66)]. Al respecto, se ha sostenido que los privados antepondrían sus propios beneficios, por lo que la autorregulación podría resultar indulgente y no necesariamente protectora de los derechos individuales. Además, se ha dicho que, en general, los procesos de elaboración de reglas y principios de autorregulación por el sector privado no resultan de un proceso transparente.

Esta circunstancia, trae aparejado que dicho proceso podría resultar no sólo perjudicial para las y los titulares de derechos sino que, también podría significar un perjuicio a competidores o posibles competidores que no participaran del programa de autorregulación del que se trate. En cuanto al último punto, la autorregulación promovida por grandes empresas puede derivar en procesos que resulten onerosos y cuyo costo sea transferido a los y las consumidoras y además puede que resulte en una barrera de entrada al mercado para nuevos competidores y negocios más pequeños con menores recursos [(67)].

Otra crítica atendible es en relación con la ejecución de las reglas y principios en cuestión, toda vez que los privados y representantes de la industria tienen pocos incentivos para aplicar multas y sancionar en caso de incumplimientos [(68)]. En algunos casos, la experiencia ha demostrado la ineficacia a la que se hace referencia más arriba. Un ejemplo que da cuenta de esto, puede observarse en el caso de la "Online Privacy Alliance", una organización creada a mediados de los 90' que establecía lineamientos de protección de datos personales a través de estos mecanismos de autorregulación. Los lineamientos propuestos por esta Alianza, no protegían a los usuarios y las usuarias contra el uso dañoso de los datos salvo a través de mecanismo de opt-out, ni prohibía la recolección

de datos personales. Además, algunas empresas que realizaban tratamientos masivos de datos, tal como Amazon.com, no formaron parte de tal alianza. Estas cuestiones, entre otras, llevaron a que algunos años después de su creación la organización misma reconociera su fracaso y apoyara iniciativas regulatorias provenientes del Estado [(69)].

Otro caso que expuso las falencias de los mecanismos de autorregulación respecto de su aplicación, indulgencia y participación de los actores de la industria que resaltan quienes critican a este mecanismo, fue el caso de "Network Advertising Initiative" (NAI). NAI no pudo superar el desafío que implicaba velar por el cumplimiento de sus lineamientos y de su aplicación [(70)].

No obstante, los mecanismos de autorregulación en mercados emergentes pueden aún resultar útiles, en particular para generar confianza de cara a las personas consumidoras y ayudarlas a distinguir entre los buenos y los malos jugadores del mercado. Además, estos mecanismos han demostrado ser eficaces para adaptarse mejor a la innovación y a los cambios tecnológicos por lo que sirven a los efectos de promover el avance normativo y cubrir posibles vacíos de implementación de normas y aún pueden servir a los efectos de la regulación eficiente [(71)]. La Organización para la Cooperación y el Desarrollo Económico (OCDE) ha concluido que la eficacia de los mecanismos de autorregulación depende principalmente de cuatro factores: 1) la solidez de los compromisos asumidos por los participantes; 2) la cobertura industrial de la autorregulación; 3) la medida en que los participantes se adhieran a los compromisos; y 4) las consecuencias de no adherirse de los compromisos [(72)]. Estos puntos pueden ser reforzados mediante regulación estatal dando lugar a esquemas híbridos de regulación como es el sistema de co-regulación.

Ante las críticas y falencias de la autorregulación, se ha propuesto como esquema superador el de la "co-regulación". Este es un término acuñado por cierta parte de la doctrina que se refiere a iniciativas regulatorias en las que participan el gobierno y la industria, compartiendo responsabilidad de redactar y aplicar normas reguladoras. Dennis D. Hirsch lo describe como un sistema regulatorio híbrido en el que se complementa la normativa emitida

por el Estado [73]. Bajo este sistema, el Estado presiona a los privados para que prioricen el bienestar general. Además, al presentar esquemas colaborativos entre privados y el gobierno se aumenta la posibilidad de intercambio de información y cooperación, lo que se traduce en normativa de mejor calidad para la ciudadanía.

Quienes se oponen a estos mecanismos de co-regulación se muestran escépticos a las supuestas ventajas del sistema y sostienen, por ejemplo, que los privados se mostrarán reticentes a develar información para obtener estándares más laxos. Sin embargo, en la actualidad se presenta como una alternativa de regulación que puede ser efectiva en términos de costos y que lleve a estándares flexibles de protección de la privacidad de los individuos [74].

Según De Mooy, un sistema de co-regulación efectivo en tiempos de tecnologías como big data y dinámicas propias del ecosistema de datos requieren de políticas públicas y regulación que incluya (i) empoderamiento de los individuos mediante educación y derechos de portabilidad; (ii) responsabilidad demostrada de parte de las empresas a través de mecanismo de autorregulación y (iii) la responsabilidad colectiva mediante el uso de evaluaciones de impacto por mandato legal [75]. Así vemos que estos tres puntos hacen a un sólido esquema de co-regulación, que se presenta como un mecanismo superador al de la autorregulación.

En relación con el Acuerdo, cabe mencionar que si bien el texto refiere a la "autorregulación" debe entenderse como una forma de co-regulación [76], ya que estos mecanismos no pretenden reemplazar a la normativa vigente, sino complementarla. Así, la promoción de estos mecanismos no debe interpretarse como excluyente de la regulación estatal o como un llamado a reemplazarla, si no como insertos en un sistema de "co-regulación".

En la región los mecanismos de autorregulación cobraron especial relevancia a fines de impulsar la regulación incipiente -o inexistente al momento de su desarrollo- y cumplimiento. Así, desde la perspectiva de la oferta (es decir, de las empresas, en particular las pymes) puede afirmarse que los mecanismos como

Sellos de Confianza colaboran con el acceso a la información y la capacitación para el cumplimiento de las mejores prácticas del mercado y de la normativa aplicable. Esto significa que las instituciones -públicas o privadas- que los promueven no lo hacen como reemplazo a la normativa vigente sino todo lo contrario: buscan capacitar a las empresas y emprendedores y emprendedoras de la región, al tiempo que les permiten demostrar a sus consumidores y consumidoras, que cumplen la ley. Asimismo, resulta relevante destacar que para la región del Mercosur, en la que las pymes juegan un rol fundamental como motor de la economía, el fomento de la autorregulación en el sector privado como complemento a la regulación estatal resulta útil para promover el cumplimiento de la ley, la confianza y la seguridad jurídica en el comercio electrónico. Esto considerando el enorme crecimiento e impulso que ha tenido el comercio electrónico en la pandemia y la cantidad de empresas, en especial pymes y emprendedores y emprendedoras, que se volcaron al canal online -muchas veces sin haber hecho todos los "deberes" antes- para poder subsistir en un contexto en el que la población se encontraba confinada en los hogares.

Entonces existen diversos factores que a lo largo de los años han volcado a las empresas, a las cámaras y asociaciones que las agrupan a considerar a los sellos de confianza como una herramienta valiosa. Entre otros, podemos mencionar:

- Contar con una hoja de ruta simplificada para operar en múltiples jurisdicciones o para facilitar el cumplimiento de la normativa y/o de estándares técnicos de la industria.
- Ofrecer certeza y transparencia a las empresas con base en otras jurisdicciones con las que se interactúa respecto del cumplimiento de normativa y estándares de la industria.
- Brindar transparencia y seguridad a los/as consumidores/as en materia de atención a clientes, resolución de reclamos, procesos de baja de cuentas o contenidos o prevención del fraude, privacidad y procesos de desindexación de datos personales, etc.
- Generar confianza en clientes, usuarios/as y consumidores/as fortaleciendo la distinción entre los "buenos jugadores" como aquellos cumplen con la normativa y los estándares de la industria del comercio electrónico, respecto de los "malos jugadores" (diferenciación de la competencia).

Ahora bien, desde la perspectiva del consumidor/a, los sellos de confianza se suelen traducir en una experiencia positiva. Ante una compra online, el consumidor o la consumidora podría preguntarse, cuestiones tales como: ¿Recibiré el producto que compré? ¿Me llegará en la fecha acordada? ¿Qué pasará con los datos de mi tarjeta de crédito que ingresé en la plataforma? ¿Podré ser víctima de un fraude? ¿Qué pasa si recibo un producto o servicio equivocado o dañado? ¿Cómo procederá la devolución y quién pagará los costos asociados al reemplazo? ¿Cómo puedo tener la seguridad de que si pongo los datos de mi tarjeta de crédito no me los van a robar? ¿Es esta empresa a la que compré la que creo que es? ¿Con quién se compartirán mis datos personales y en qué me podría perjudicar esta situación?

Los códigos de conducta y los sellos de confianza están pensados para informar en forma estandarizada y clara, mediante un lenguaje comprensible y amigable. La forma de organizar la información y de comunicar muchas veces hace la diferencia para la generación de confianza del usuario/a y/o consumidor/a. Estos marcos de confianza se ofrecen a través de cámaras empresarias u otras asociaciones, o por empresas privadas que funcionan con el rol de brindar servicios de "terceros de confianza". Asimismo, estos esquemas pueden surgir como iniciativas público-privadas, lo que presenta mejores perspectivas de éxito como modelo para el intercambio comercial transfronterizo, pudiendo operar a nivel local, regional, transatlántico o incluso global. Las empresas adhieren a ellos de forma voluntaria, siendo que contienen normativa aplicable o una versión armonizada de la normativa en diversos países, estándares técnicos, reglas éticas y buenas prácticas de la industria.

La adhesión a los mecanismos referidos se suele llevar a cabo mediante diferentes clases de procesos, ya sea autogestivos o por medio de auditorías automatizadas o no. En algunos casos, las empresas menos experimentadas buscan en estos mecanismos una guía que funcione al estilo de un check-list u hoja de ruta para salir a vender online por primera vez o para acceder a nuevos mercados, pudiendo hacerlo con la tranquilidad de estar en cumplimiento de la normativa aplicable en dichas jurisdicciones. Por lo general los procesos de adhesión requieren la inclusión de la razón social o marca de la empresa

en un listado de algún sitio web donde figuran las compañías adheridas y la información del Código de Conducta - o similar- del que se trata, e incluso con acceso a mecanismos de denuncia o reclamación en línea [(77)]. Generalmente, se entregará a la empresa un sello (una imagen o logotipo asociada a un enlace) para que lo coloque en sus propios sitios o aplicaciones. Esto derivará a los usuarios y las usuarias al sitio web del "tercero en confianza" donde consta la información del sistema del que se trate y de la empresa adherida. Los sellos de confianza o certificaciones similares servirán además como una forma de diferenciación, posicionamiento y generación de confianza en la clientela y/o la audiencia de la empresa adherida. Al enlazar con el sitio de un tercero confiable (como una cámara o asociación industrial) se dará cuenta de que la compañía adherida es legítima y ha pasado por algún proceso de certificación que da cuenta de que cumple con los estándares propuestos por dicho tercero, que normalmente incluirán el cumplimiento de la regulación aplicable. En algunos casos se ofrecerán otros servicios asociados a los sellos.

En relación con las cuestiones de privacidad y protección de datos personales, es interesante traer a colación el ejemplo del caso de los Sellos de Confianza sobre Protección de Datos Personales ofrecidos por la Asociación Mexicana de Internet que nacieron en el 2007. Si bien México no es Estado parte del Mercosur, su comercio electrónico es similar al de los países más grandes del bloque, y su experiencia en este y otros ámbitos sirve igualmente como ejemplo regional. En ese caso, se trató de una iniciativa del sector privado mexicano en cooperación con el sector público que buscaba el fomento del crecimiento del comercio electrónico en dicho país mediante la autorregulación para generar confianza en materia de privacidad ante la ausencia, en ese entonces, de normativa sobre protección de datos personales. La normativa mexicana finalmente fue dictada algunos años después ya con la experiencia ganada y el músculo del sector privado entrenado, conformando así un ejemplo de co-regulación.

Los Sellos de Confianza en México se pusieron en marcha en 2007, con base en el Marco de Privacidad de APEC (en inglés, APEC Privacy Framework) y de ese modo, como relata su propia web, "la Asociación de Internet en colaboración

directa con la Secretaría de Economía, a través del Programa para el Desarrollo de la Industria del Software (PROSOFT), y en su afán por promover las mejores prácticas en línea en México, crearon y ejecutaron el proyecto de Sellos de Confianza Asociación de Internet.mx®, un mecanismo de autorregulación en materia de privacidad, enfocado principalmente al mercado digital"[(78)]

En una etapa en que México carecía de normativa específica sobre esta temática, este proyecto evolucionó favorablemente incluyendo la regulación que finalmente fue dictada allí. En la actualidad, la Asociación Mexicana de Internet sigue promocionando los Sellos de Confianza como distintivos que brinda a sitios web de empresas, organizaciones y personas humanas que han sido evaluadas y que cumplen con determinados requisitos, incluyendo, desde ya, la normativa vigente. Todo ello con el objetivo de la generación de confianza. Cabe mencionar que este sistema convive y se complementa con la regulación del Estado, por lo que podemos considerarlo actualmente como un modelo de co-regulación.

En esta misma línea, en la región se han desarrollado otros modelos de autorregulación y co-regulación basados en sellos de confianza que por ejemplo, proveen códigos de conducta. Así, podemos mencionar el esquema de la iniciativa de Sellos de Confianza del Instituto Latinoamericano de Comercio Electrónico o actualmente eCommerce Institute que brindaba un código de conducta en el que se incluían disposiciones de protección de datos personales inspiradas en la normativa vigente en Argentina [(79)]. Este código ha sido aprovechado para generar conciencia en las pymes de la región respecto de la normativa aplicable, en un contexto en el que no siempre las Autoridades de Control se dedicaron al enforcement activo de las empresas de retail y la población no se encontraba lo suficientemente informada respecto de sus derechos, en materia de protección de datos personales.

En el 2012 la iniciativa eConfianza mencionada lanzó junto con la Cámara Argentina de Comercio Electrónico una versión específicamente desarrollada para empresas de Argentina de dichos sellos, que fueron denominados "Sellos CACE". Estos eran adoptados por las empresas socias de la cámara, que eran

capacitadas en materia de generación de confianza en los y las consumidoras por medio del cumplimiento de los aspectos legales del comercio electrónico y la demostración activa de dicho cumplimiento como estrategia de diferenciación en el mercado. Las empresas que aprobaban el proceso de certificación, accedían a incluir su marca en el listado de compañías adheridas en el sitio web del Sello CACE, en donde cada marca contaba con un "perfil" con información disponible de la empresa, de cara al consumidor/a, entre otros servicios.

Tanto los sellos eConfianza, que apuntaban a empresas de la región, como los Sellos CACE, que apuntaban a empresas de Argentina, contaban con un Código de Conducta que incluía una sección específica sobre la cuestión de la protección de datos personales que replicaba la normativa vigente y los estándares internacionales en la materia [(80)].

En la misma línea, podemos situar al Código de Ética de la Asociación de Marketing Directo e Interactivo de Argentina (en adelante "AMDIA") que fuera homologado por la Disposición 4/2004 de la Dirección Nacional de Protección de Datos Personales y que contiene normativa y reglas de conducta en materia de protección de datos personales, especialmente enfocadas en la labor de las empresas que realizan marketing directo en Argentina [(81)].

Este tipo de iniciativas fueron muy relevantes para el sector, brindando definiciones para temas que no se encontraban específicamente definidos o regulados en la normativa al momento, y llevando claridad al sector del marketing directo como industria pujante y en permanente desarrollo.

Entendemos que, al día de hoy, el avance de la regulación en materia de comercio electrónico y protección de datos personales en la región hizo que este tipo de mecanismos funcionen no tanto como mecanismos de autorregulación sino como esquemas de "co-regulación". Esto último refiere a que los sellos de confianza conviven y replican en sus códigos de conducta la normativa dictada y aplicable, reforzando los esfuerzos de implementación y cumplimiento de las normas vigentes por parte del sector privado, en beneficio de los consumidores y las consumidoras. En algunos casos, incluso pueden ir

más allá e incluir estándares técnicos o de calidad. En este sentido, mientras la legislación establece normas de cumplimiento obligatorio, los esquemas de los sellos de confianza funcionan como una guía interpretativa práctica para la implementación y el cumplimiento de lo regulado. Sumado a ello, los sellos, como se ha mencionado, sirven para evidenciar el cumplimiento de las normas con el objetivo de generar confianza (como parte de estrategias de marketing). Por último, estos mecanismos traen luz a los espacios no cubiertos por la norma cuando se utilizan en el marco de industrias específicas con avances tecnológicos dinámicos y cambiantes.

Otro modelo interesante y nuevo, es el del sello de confianza de la Procuraduría Federal del Consumidor del Gobierno de México (en adelante "Profeco") que ofrece un sello denominado Distintivo Digital. Este tiene como objetivo funcionar como un reconocimiento oficial que se otorga a aquellas empresas proveedoras de bienes, productos o servicios que se destaquen por promover y favorecer estándares elevados en materia de comercio electrónico, tales como información clara y completa, seguridad, transparencia, confidencialidad, confianza y certeza jurídica a favor del consumidor/a. El esquema del Distintivo Digital de Profeco ofrece que cada empresa adherida cuente con su propio Código de Ética que puede descargarse del sitio del Distintivo Digital. El Código de Ética, según se lo describe "es un conjunto de valores y principios que todo proveedor adherido deberá observar en las actividades relacionadas con el comercio electrónico, a fin de respetar y promover los derechos de la población consumidora, fomentar una cultura de consumo responsable, la protección de grupos vulnerables y la autorregulación" (82).

En definitiva, se trata de un conjunto de normas mínimas que las empresas adheridas deciden voluntariamente comprometerse a cumplir para que las compras online que se realizan en sus sitios se efectúen "en un marco de respeto a los derechos de los consumidores, adoptado el uso de herramientas y las mejores prácticas comerciales a nivel global" (83). El código contendrá estándares mínimos considerados como requisitos de adhesión, entre los cuales destacamos: información acerca el tratamiento que se dará a los datos personales proporcionados por los consumidores a través del Aviso

de Privacidad; requisitos asociados a la protección de los niños, niñas y adolescentes; protección de los grupos vulnerables; fomento de los mecanismos específicos y alternativos para resolución de conflictos y dudas, exigiéndose como estándar el actuar de forma diligente en los procedimientos conciliatorios para llegar a acuerdos con el propósito de beneficiar a los consumidores; e implementación de la empresa de mecanismos de verificación de cumplimiento de lo declarado en dicho código [(84)].

Es interesante tener en cuenta que el proceso de adhesión implica una revisión por parte de Profeco para verificar si los postulantes cumplen con los requisitos del esquema del Distintivo Digital. Este proceso incluye la posibilidad de que Profeco emita observaciones para que el postulante subsane cualquier falta, previo a obtener la aprobación. Una vez aprobado, se concede el derecho de obtener el registro y eventualmente el reconocimiento para poder estar enlistado en el sitio del Distintivo Digital como empresa cumplidora.

Por último, este tipo de esquemas conocidos como de "co-regulación", en los que participan las empresas y el Estado, nos lleva a pensar en la posibilidad de contar con mecanismos análogos que sean útiles para el respeto de la regulación y la generación de confianza a nivel del comercio electrónico transfronterizo. En especial, podría resultar útil para asegurar un flujo transfronterizo de datos en cumplimiento de estándares mínimos en materia de derechos de los consumidores y de protección de datos personales. Por ejemplo, podría pensarse en que habiendo los Estados sentado los presupuestos mínimos de protección de datos personales por medio de la regulación, puedan luego desarrollarse entidades certificantes avaladas por ellos, como sucede en el caso del acuerdo de reconocimiento de firma digital. A su vez estas entidades certificantes estarían en condiciones de acreditar a las empresas que voluntariamente se adhirieron a dicho marco regulatorio para demostrar el cumplimiento de los presupuestos mínimos de protección establecidos por la normativa estatal. Además, se podría permitir incluso que las empresas decidan voluntariamente elevar dichos estándares en beneficio de sus clientes/as, usuarios/as y consumidores/as. En tal supuesto, no sólo se garantizaría el cumplimiento de la normativa por los actores sino que además,

al incluir el sello o certificado de distinción, se haría visible a las empresas entre sí y a los consumidores tal estándar de cumplimiento generando confianza (la cual, como venimos diciendo, constituye un eslabón esencial para el desarrollo del comercio electrónico en la región).

Todo lo anterior se complementa con la tendencia normativa actual en materia de protección de datos personales que reconoce la capacidad de los privados para establecer marcos normativos que cumplan con los estándares de protección de los y las titulares de los datos requerido por la ley bajo sistemas de co-regulación.

4. El Acuerdo y el marco regulatorio local en los Estados Parte (Argentina, Brasil, Paraguay y Uruguay)

En esta sección analizaremos en detalle los marcos regulatorios locales de los Estados parte y los compararemos con los preceptos establecidos en el Acuerdo. Las características de dichos marcos regulatorios pueden resumirse en el siguiente cuadro:

	Argentina	Brasil	Paraguay	Uruguay
Marco normativo local que respeta los estándares internacionales de protección de datos	✓	✓	✖	✓
Consentimiento como base legal del tratamiento	✓	✓	✓	✓
Principio de finalidad	✓	✓	✓	✓
Principio de calidad	✓	✓	✓	✓
Régimen de Responsabilidad (penalidades por incumplimiento)	✓	✓	✖	✓
Regulación en materia de medidas de seguridad	✓	✓	✓	✓
Régimen de transferencias internacionales	✓	✓	✓	✓
Regulación apropiada en materia de comunicaciones comerciales directas no solicitadas	✖	✓	✖	✖

A continuación, analizaremos en detalle la normativa de cada uno de los Estados parte.

4.1. Argentina

El marco regulatorio en materia de protección de datos personales en Argentina se alinea a las disposiciones en dicha materia que se han receptado bajo el Acuerdo, por lo que posiblemente su adopción no requiera de cambios sustanciales en la regulación local actual.

Resumidamente, podría afirmarse que en lo que refiere específicamente a la regulación de la protección de datos personales, el Acuerdo establece obligaciones respecto de los siguientes puntos: (i) prever un marco normativo en la materia que cumpla con los estándares internacionales, la que deberá contener principios generales tales como el previo consentimiento, finalidad, calidad, seguridad, responsabilidad, entre otros; (ii) medidas de seguridad; (iii) transferencias internacionales; y (iv) comunicaciones comerciales directas no solicitadas. A continuación, se analizan estos puntos en detalle:

4.1.1. Marco normativo en la materia que cumpla con los estándares internacionales, que deberá contener principios generales tales como el previo consentimiento, finalidad, calidad, seguridad, responsabilidad, entre otros.

En Argentina el régimen de protección de datos personales está regulado principalmente por la Ley de Protección de Datos Personales Nº 25.326 (en adelante "LPDPA"), su Decreto Reglamentario 1558/2001, toda su normativa reglamentaria y complementaria, así como aquella que ha emitido la autoridad de aplicación (actualmente la Agencia de Acceso a la Información Pública y antes de la entrada en vigencia del Decreto N° 899/2017, la Dirección Nacional de Protección de Datos Personales).

La LPDPA establece, bajo su capítulo II, los principios generales relativos a la protección de datos personales que rigen su tratamiento siendo estos principios los siguientes: (i) licitud; (ii) calidad de los datos y finalidad; (iii) consentimiento; (iv) información; (v) categoría de datos; (vi) datos relativos a la salud; (vi) seguridad de los datos; (vii) confidencialidad; (viii) cesión; y (ix) transferencia internacional.

El principio de licitud requiere que los responsables del tratamiento registren las bases de datos ante la autoridad de aplicación, las que deberán operarse conforme a la ley y no deberán tener finalidades contrarias a esta ni a la moral pública. Esta obligación de registro, que no se encuentra bajo el Acuerdo analizado, es objeto de críticas por su utilidad y los últimos proyectos de ley que han sido presentados en la materia dispensan de tal obligación a los responsables de tratamiento [(85)].

El principio de calidad de los datos, previsto bajo el artículo 4 de la LPDP, contiene también el de finalidad en tanto que requiere -entre otras cuestiones- que (i) los datos recolectados sean ciertos, adecuados, pertinentes y no excesivos en relación con el ámbito y finalidad para los que se hubieren obtenido [(86)]; y (ii) que los datos no sean utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención [(87)].

Bajo la LPDPA se establece un esquema de obligaciones en cabeza de los responsables (denominados controllers en la legislación comparada) y encargados del tratamiento (denominados processors) de los datos personales, previendo incluso la responsabilidad solidaria entre éstos, ante el o la titular de los datos de los datos, en caso de incumplimiento a sus obligaciones respectivas [(88)].

Por último, Argentina es considerada aún jurisdicción adecuada bajo normativa europea. En virtud de ello, podría afirmarse que cumple con los estándares internacionales a los que se refiere el artículo [(89)]. Al respecto, cabe mencionar que al entrar en vigor el Reglamento General de Protección de Datos Personales Europeo (Reglamento UE 2016/679) se inició un nuevo proceso de revisión de

los niveles de adecuación de cada jurisdicción, estando Argentina alcanzada por este. Sin perjuicio de lo anterior, la Agencia de Acceso a la Información Pública (en adelante "AAIP") emitió diferentes resoluciones para adecuar la normativa vigente a los estándares de la regulación europea [(90)] y se espera que, eventualmente, ante una reforma de la normativa actual, se siga esa misma línea para mantener el estatus de país adecuado.

4.1.2. Medidas de seguridad

La LPDPA regula bajo su artículo 9 la obligación de implementar medidas de seguridad estableciendo que el sujeto obligado bajo dicha norma "...debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado" [(91)]. Además, prohíbe el registro y tratamiento de datos en bases de datos que no reúnan condiciones técnicas de integridad y seguridad [(92)]. Con relación a este punto, la AAIP emitió medidas de seguridad recomendadas para el cumplimiento de esta obligación de seguridad mediante la Resolución 47/2018, las que si bien no son estrictamente vinculantes para los sujetos obligados, pueden interpretarse como un piso mínimo que debe alcanzarse. Cabe destacar que el cumplimiento de las medidas de seguridad se interpretará conforme el particular tratamiento que realiza el responsable y el estado de la técnica al momento de su evaluación.

4.1.3. Transferencias internacionales

Las transferencias internacionales de datos personales se encuentran especialmente reguladas bajo el régimen de protección de datos personales en Argentina. Así, en principio, el artículo 12 de la LPDPA [(93)] prohíbe la transferencia de datos personales a jurisdicciones que no garanticen niveles adecuados de protección conforme la regulación vigente [(94)], siendo la Autoridad de Control (la AAIP) competente para evaluar el cumplimiento de este estándar.

No obstante, el mismo artículo 12 establece seguidamente excepciones a dicha prohibición, como el supuesto de tratados internacionales en los que sea parte la Argentina [(95)] o cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico [(96)], entre otros. Además, el Decreto Reglamentario 1558/2001 prevé que los niveles adecuados de protección a los que refiere la ley podrán provenir directamente del ordenamiento jurídico vigente, sistemas de autorregulación o de cláusulas contractuales que prevean la protección de datos personales. Los últimos dos supuestos reconocen la facultad de los privados de establecer un marco regulatorio que cumpla con el estándar requerido y han sido específicamente regulados por la Autoridad de Control.

En lo que respecta a los sistemas de autorregulación, la AAIP emitió la Resolución 159/2018 que establece lineamientos y contenidos básicos que deberán contener las normas de autorregulación entre empresas de un mismo grupo económico (conocidas como Normas Corporativas Vinculantes o por su nombre y sigla en inglés, Binding Corporate Rules, en adelante "BCRs") para cumplir con los niveles de adecuación que se requieren bajo la normativa local [(97)]. En el supuesto de que tales normas se aparten de los lineamientos emitidos por la Autoridad de Control, la transferencia de datos quedará supeditada a la aprobación por parte de esta última.

Las cláusulas contractuales que adopten las partes para transferir datos personales a jurisdicciones que no garanticen niveles adecuados de protección se encuentran reguladas bajo la Disposición 60E/2016 emitida por la entonces Dirección Nacional de Protección de Datos Personales [(98)]. Esta Disposición contiene cláusulas modelo que son concebidas como el piso mínimo que debe garantizar el documento que se ejecute entre las partes contratantes, a los fines de la transferencia en cuestión. Tal y como fuera mencionado para el caso de las BCRs, en el supuesto que se utilicen contratos que difieran de las cláusulas aprobadas o no contengan los principios, garantías y contenidos relativos a la protección de los datos personales previstos en los modelos aprobados, previo a la transferencia de los datos se deberá solicitar la aprobación ante la Autoridad de Control.

4.1.4. Comunicaciones comerciales directas no solicitadas

En principio, la base legal para el tratamiento de datos personales con fines de publicidad bajo la normativa argentina, es el consentimiento del titular. Recordemos en este sentido que la norma de protección de datos argentina establece en su artículo 5.1 que el consentimiento debe ser "libre, expreso e informado, y deberá constar por escrito, o por otro medio que permita que se le equipare, de acuerdo a las circunstancias" y brinda en el artículo 5.2 las pocas excepciones en las cuales no se requiere el consentimiento. A su vez, el artículo 6 establece la obligación de informar previamente o al momento de la recolección, a los titulares de datos, en forma expresa y clara, respecto de: la finalidad del tratamiento; la identidad y domicilio del responsable de la base de datos en la cual serán tratados sus datos personales; y la posibilidad del interesado de ejercer sus derechos de acceso, rectificación y supresión.

No obstante, bajo la reglamentación del artículo 27 de la LPDPA a través del Decreto Reglamentario 1558/2001[(99)] se ha interpretado que existe una excepción al requerimiento del consentimiento para ciertos tratamientos de datos con fines de publicidad. Tal es así, que se dispensa del consentimiento del titular para tratar, recolectar y ceder datos que sean aptos para la formación de perfiles determinados, que categoricen preferencias y comportamientos similares de las personas.

Siempre que los titulares de los datos sólo se identifican por su pertenencia a tales grupos genéricos, con los datos individuales estrictamente necesarios para formular la oferta a los destinatarios. En tales casos, y en general, para toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, internet y otro medio a distancia, la norma establece, en primer lugar, que se debe indicar en forma expresa y destacada el derecho del titular a solicitar el retiro o bloqueo total o parcial de su nombre de la base de datos, es decir, el principio del opt-out ya referido. Dicho artículo también indica que el titular tendrá derecho a solicitar que se le informe el nombre del responsable de la base de datos que proveyó su información.

Por su parte, la Disposición 4/2009 [100] indica con más precisión cómo debe informarse el derecho de retiro o bloqueo en las comunicaciones con fines de publicidad. Agregando que para el caso de las comunicaciones con fines de publicidad directa no solicitadas o no requeridas por el titular del dato se indique que se trata de una publicidad, insertándose dicho término en su encabezado, en el caso que sea mediante correo electrónico.

Cabe mencionar que bajo la normativa argentina se entiende que las excepciones al consentimiento, las que en este caso además están previstas por la reglamentación a la ley y no por la propia norma, deben entenderse de forma restrictiva. En este sentido, entendemos que tanto la tendencia normativa como la industria del email marketing se dirigen hacia esquemas de opt-in, es decir, en los cuales se requiere el consentimiento previo de los titulares para el envío de comunicaciones de publicidad. En línea con esto último, se observa que las excepciones al consentimiento para comunicaciones de publicidad no solicitadas se restringen, como sucede en el caso del proyecto de acuerdo entre Mercosur y Unión Europea referido en este trabajo, que sólo las habilita para el caso de relaciones previas con el consumidor y respecto de productos o servicios contratados por ese.

En caso de entrar en vigor el Acuerdo, la regulación de la normativa argentina se deberá adecuar, en tanto no se permiten las comunicaciones no solicitadas, salvo por el supuesto referido en el párrafo anterior.

En este sentido, la excepción al consentimiento prevista por el artículo 27 del Decreto Reglamentario 1558/2001 y específicamente regulada por el Decreto 4/2009 para comunicaciones de publicidad directa no solicitadas, ya no estaría facultada para los casos previstos por la regulación argentina de formación de perfiles. Y debería circunscribirse, en cambio, al caso de relaciones previas con el consumidor (el Acuerdo dice textualmente "en el marco de la venta de un producto o servicio", lo que podría generar ciertas discrepancias interpretativas respecto de si dicho consumidor debe ser "cliente" o no, y si el marco de la "venta" se refiere a un contrato completo ejecutado, o simplemente a la oferta de venta).

4.2. Brasil

El 1 de agosto de 2021 entró en vigor en Brasil la Ley General de Protección de Datos Personales No. 13.709, sancionada el 14 agosto de 2018 ("LGPDP") que sigue las últimas tendencias normativas en la materia y que guarda similitudes con el Reglamento General de Protección de Datos Personales Europeo (Reglamento UE 2016/679).

4.2.1. Marco normativo en la materia que cumpla con los estándares internacionales, que deberá contener principios generales tales como el previo consentimiento, finalidad, calidad, seguridad, responsabilidad, entre otros.

La regulación de protección de datos personales en Brasil establece que el procesamiento de estos debe llevarse a cabo de buena fe y siguiendo diez principios fundamentales. Estos principios son: finalidad, adecuación, necesidad, libre acceso, calidad, transparencia, seguridad, prevención, no discriminación y responsabilidad demostrada.

El principio de finalidad establece que el procesamiento de datos debe hacerse conforme al propósito legítimo, específico y explícito que fue consentido por el titular del dato, estando prohibido un tratamiento incompatible con dicho propósito [(101)]. Éste se complementa con el principio de adecuación que establece que la finalidad del procesamiento no sólo debe ser debidamente comunicada al titular, si no que además debe ser adecuado conforme su contexto [(102)] y con el principio de necesidad (también conocido como "principio de minimización") [(103)]. Bajo el principio de minimización los datos recolectados deben ser sólo aquellos que sean relevantes, proporcionales y no excesivos en relación a la finalidad del tratamiento en cuestión.

En lo que refiere a la calidad, la normativa brasileña establece que los datos deben ser adecuados, claros, relevantes y actualizados conforme el propósito de su procesamiento [(104)].

La LGPDP adopta el principio de responsabilidad demostrada (“accountability”), principio que requiere que los sujetos obligados puedan evidenciar ante la autoridad competente y/o terceros su cumplimiento con la regulación aplicable, incluyendo la eficacia de las medidas que han adoptado conforme a la misma [(105)].

El esquema de responsabilidad de los agentes que intervienen en el procesamiento de los datos personales se encuentra regulado bajo la sección III del Capítulo VI. Así, se establece la obligación de remediar en caso de daños producidos por el incumplimiento a la normativa en cuestión y se garantiza la compensación a los titulares de datos afectados, al prever la responsabilidad solidaria frente a titular, entre procesadores y responsables que intervengan en el tratamiento, si los primeros incumpliesen las instrucciones de los últimos [(106)].

El consentimiento del titular es un requisito imprescindible para el procesamiento legítimo de sus datos personales, que se encuentra especialmente regulado [(107)]. Entre otros requisitos, se requiere que el consentimiento sea otorgado para los fines particulares -siendo inválidos aquellos que se otorgan de forma genérica [(108)]- y sea escrito o por medios asimilables, siendo el responsable del tratamiento quien debe probarlo [(109)].

4.2.2. Medidas de seguridad

La LGPDP establece bajo el capítulo VII que se regula específicamente la obligación de seguridad y las buenas prácticas en el procesamiento de datos personales [(110)]. Siguiendo el principio de seguridad, el procesamiento de los datos personales debe ejecutarse bajo medidas técnicas y administrativas que protejan la información de accesos no autorizados y de situaciones accidentales o ilegales de destrucción, pérdida, adulteración, comunicación o diseminación. Las medidas de seguridad deberán ser acordes a la naturaleza de la información procesada - en especial si se trata de datos sensibles-, las características particulares del procesamiento y el estado de la técnica.

Además, la LGPDP faculta a la autoridad de control para establecer estándares de seguridad mínimos que deberán adoptar los responsables (controllers) y los procesadores (processors) en el tratamiento de datos personales [(111)]. Por último, cabe destacar que el incumplimiento de los estándares de seguridad regulatorios se considera bajo esta normativa como un supuesto de responsabilidad [(112)].

4.2.3. Transferencias internacionales

Las transferencias internacionales de datos se encuentran reguladas bajo el capítulo V de la LGPDP estableciendo los supuestos en los que se habilitan. Estos son:

- cuando se transfieren datos a países u organizaciones internacionales que proveen niveles de protección adecuados conforme la legislación brasileña;
- cuando el responsable ofrece y garantiza el cumplimiento con los derechos de los titulares de los datos y la legislación (lo que puede ser en forma de cláusulas específicas para una transferencia en particular; cláusulas modelos; normas corporativas vinculantes; y/o sellos, certificaciones o códigos de conducta);
- cuando el titular de los datos haya prestado su consentimiento específico para la transferencia internacional en cuestión;
- cuando sea necesaria para la cooperación jurídica internacional entre los organismos públicos de inteligencia, investigación y fiscalía, de conformidad con los instrumentos de derecho internacional; entre otros supuestos taxativamente previstos en la ley [(113)].

El nivel adecuado de protección de un país o de un organismo internacional estará dado por la Autoridad de Aplicación, tomando en consideración aspectos tales como la legislación vigente en el país de destino; la naturaleza de los datos; el cumplimiento de los principios generales para la protección de datos personales previsto en la LGPDP. Además, la adopción de medidas de seguridad; la existencia de garantías judiciales e institucionales para garantizar tales derechos; y otras circunstancias relativas a la transferencia.

Asimismo, la Autoridad de Aplicación será quien determine los contenidos que deben prever los mecanismos que habilitan la transferencia internacional de datos personales (las cláusulas modelos, normas corporativas vinculantes; y/o sellos, certificaciones o códigos de conducta, etc) [(114)] y quien verifique el cumplimiento de tales estándares en los acuerdos específicos.

4.2.4. Comunicaciones comerciales directas no solicitadas

En principio, las comunicaciones directas no solicitadas no están permitidas bajo la LGPDP, en tanto el consentimiento es requisito esencial para el tratamiento legítimo de datos [(115)]. Por esto, el titular del dato debería haber consentido en primer término recibir las comunicaciones comerciales.
Sin perjuicio de lo anterior, tal como se ha interpretado para el caso de la regulación europea, el consentimiento para recibir este tipo de comunicaciones puede entenderse implícito cuando existe una relación contractual previa con el consumidor, siempre que el contenido de las mismas esté relacionado al producto o servicio que se haya contratado [(116)]. En este sentido, la normativa brasileña actual se encuentra alineada con el Acuerdo analizado por lo que al entrar en vigor no será necesaria la adecuación del país en este sentido.

4.3. Paraguay

Paraguay no cuenta con un régimen integral de protección de datos personales, siendo regulada actualmente por la Ley Nº 6534 de Protección de Datos Personales Crediticios [(117)]. Sin perjuicio del nombre de la ley, esta normativa incluye disposiciones que comprenden los datos personales entendidos como "información de cualquier tipo, referida a personas jurídicas o personas físicas determinadas o determinables" [(118)].

4.3.1. Marco normativo en la materia que cumpla con los estándares internacionales, que deberá contener principios generales tales como el previo consentimiento, finalidad, calidad, seguridad, responsabilidad, entre otros.

El marco normativo de Paraguay previsto bajo la Ley Nº 6534 se centra principalmente en los datos crediticios y en la regulación aplicable a quienes prestan servicios de esta índole, por lo que puede decirse que en caso de que el Acuerdo entre en vigencia, el país deberá adecuar su regulación [(119)].

El consentimiento es la base legal para el tratamiento de datos personales bajo la regulación paraguaya, toda vez que el artículo 6 establece: "El tratamiento y la cesión de datos personales son ilícitos cuando el titular de los datos no hubiere prestado su consentimiento libre, expreso y consciente.". Además, cabe mencionar que el consentimiento debe ser "...expreso e inequívoco, en condiciones que no admitan dudas de su otorgamiento y deberá constar de manera escrita, electrónica, digital u otro mecanismo fehaciente". Bajo este mismo artículo podría decirse que existe cierta recepción del principio de finalidad en tanto se reconoce el derecho del titular de ser informado respecto a para qué se recolectan los datos.

El principio de calidad del dato se recepta expresamente bajo el artículo 7 de la referida norma, que indica que "los datos personales recolectados o almacenados deberán ser lícitos, exactos, completos, veraces y actualizados para el fin específico para los que fueron recolectados". Por último, la norma recepta la obligación de implementar medidas de seguridad que deberán ser "...necesarias para salvaguardar el acceso y la integridad de los datos personales, a fin de evitar su alteración, pérdida, consulta, comercialización o acceso no autorizado" [(120)].

4.3.2. Comunicaciones comerciales directas no solicitadas

Bajo el artículo 6 de la Ley Nº 6534 se establece el consentimiento como base para el tratamiento legítimo y no se prevén excepciones, por lo que podría concluirse en principio que las comunicaciones directas no solicitadas no

están permitidas bajo la regulación paraguaya. Sin embargo, la Ley Nº 4868 sobre Comercio Electrónico [121] regula la materia expresamente y dispone que los proveedores podrán enviar este tipo de comunicaciones si cumplen los siguientes requisitos: i) indicar expresamente la calidad de comunicación comercial no solicitada; ii) incluir en el mensaje un sistema fácil de exclusión de las listas de destinatarios del mismo (lo que se conoce como derecho de oposición u opt-out); iii) obtener los datos de los destinatarios sin infringir los derechos de privacidad de los mismos; y iv) establecer que la comunicación no tenga un tamaño mayor al fijado por la autoridad normativa de la ley, pudiendo incluir en la misma enlaces a información complementaria sobre la oferta [122].

4.3.3. Transferencia internacional

La Ley Nº6534 en su artículo 21 dispone como supuesto de infracción: "La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en esta Ley.". Sin embargo, por el momento no hay regulación específica que determine criterios para determinar el cumplimiento con lo allí dispuesto.

4.4. Uruguay

El régimen de protección de datos personales en Uruguay está regulado principalmente bajo la Ley de Protección de Datos Personales No. 18.331[123], promulgada el 11 de agosto de 2008 (en adelante "LPDPU") y su decreto reglamentario 414/009 [124]. Puede decirse que en 2018 Uruguay emprendió un proceso de modernización de su regulación en la materia alineada a la normativa europea. En este sentido, se advierte la incorporación a través de la Ley 19.670 [125] de disposiciones específicas que determinan la aplicación de la LPDPU, la obligación de notificación de vulneraciones de seguridad, el principio de responsabilidad, la Resolución 32/020 que prevé criterios para la designación del Delegado de Protección de Datos Personales [126] y la reciente ratificación del Convenio 108+ [127].

4.4.1. Marco normativo en la materia que cumpla con los estándares internacionales, que deberá contener principios generales tales como el previo consentimiento, finalidad, calidad, seguridad, responsabilidad, entre otros.

Tal como se adelantaba en el apartado anterior, Uruguay se encuentra en un proceso de modernización de su regulación en materia de protección de datos personales. Además, previo a esto el país ya era considerada jurisdicción con legislación adecuada para Europa. En consecuencia, puede señalarse que, en líneas generales, su regulación cumple con los estándares internacionales a los que se refiere el Acuerdo. Si bien Europa se encuentra revisando dicha adecuación, tal como con Argentina, aún no se ha emitido ninguna decisión que la modifique.

La LPDPU prescribe ciertos principios bajo el capítulo II que deben regir el tratamiento, estos son: i) valor y fuerza; ii) principio de legalidad; iii) principio de veracidad; iv) principio de finalidad; v) previo consentimiento informado; vi) seguridad de los datos; vii) reserva; y viii) responsabilidad [(128)].

El primero refiere básicamente a la obligación de los responsables del tratamiento de datos y a quienes intervienen en el mismo a respetar el resto de los principios y que estos sirvan como guía en la interpretación de la aplicación de la norma [(129)]. En lo que respecta al principio de legalidad, tal como sucede en el caso de Argentina, el mismo refiere a la obligación de registro [(130)].

El principio de veracidad requiere que los datos personales que se recaben sean veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido [(131)]. Por su parte, el principio de finalidad restringe el uso de los datos recolectados en el sentido de que sólo podrían utilizarse para el fin que motivó la recolección y que cumplido el mismo deberán suprimirse [(132)].

El artículo 9 de la Ley de Protección de Datos Personales establece como base legal para el tratamiento el consentimiento que debe ser prestado de manera

libre, previa, informada y expresa. Sin embargo, el mismo artículo establece ciertas excepciones al consentimiento, entre las que se encuentran los datos que provengan de fuentes públicas de información o que deriven de una relación contractual del titular de los datos y sean necesarios para su desarrollo y cumplimiento.

El artículo 10 de la ley consagra el principio de seguridad de los datos requiriendo a los responsables y a quienes intervengan en su tratamiento medidas para garantizar la seguridad y confidencialidad de los datos personales. Estas medidas tienen por objeto evitar la adulteración, pérdida, consulta o tratamiento no autorizado, y detectar desviaciones de información. A su vez, este principio se complementa con el de reserva que obliga a guardar confidencialidad de los datos tratados y prohíbe su divulgación a terceros [(133)].

Por último, el principio de responsabilidad está dispuesto en el artículo 12, donde se disponen medidas técnicas y organizativas apropiadas para el ejercicio de una responsabilidad proactiva.

4.4.2. Comunicaciones comerciales directas no solicitadas

Si bien el consentimiento es por defecto la base legal para el tratamiento legítimo bajo la regulación uruguaya, la redacción del artículo 21 que regula el tratamiento de los datos con fines de publicidad habilitaría el envío de comunicaciones comerciales directas no solicitadas. Lo anterior en tanto se dispone que "se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento". Tal como se refería para el caso de Argentina en caso de aprobarse el Acuerdo, bajo la regulación local deberán limitarse los supuestos que habilitan este tratamiento.

4.4.3. Transferencia internacional

El artículo 23 de la Ley 18.331 prohíbe expresamente la transferencia internacional de datos personales de cualquier tipo con países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo a los estándares del derecho internacional o regional en la materia. Sin embargo, como sucede en el caso de Argentina y Brasil, el estándar de protección puede cumplirse mediante cláusulas contractuales apropiadas que ofrezcan garantías suficientes respecto a la protección de los derechos de los titulares.

Además, la LPDPU prevé ciertos casos en los que la prohibición mencionada no rige, como sucede cuando se trate de cooperación judicial internacional, transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable, y acuerdos en el marco de tratados internacionales en los que Uruguay sea parte, entre otros.

5. El Acuerdo y otros instrumentos internacionales en materia de datos personales y economía digital

Es interesante analizar el Acuerdo en relación con otros instrumentos internacionales. En su texto evoca directamente a "principios generales" en materia de datos personales (art. 2.5.(f), pero para dilucidar el contenido de estos, no sólo es importante evaluar las legislaciones nacionales de los Estados parte, sino también revisar el contenido de diversos instrumentos internacionales que los rigen, tales como el Convenio N°108 del Consejo de Europa y los Estándares de Protección de Datos de los Estados Iberoamericanos. Por otro lado, es importante destacar las similitudes de este, con el Acuerdo de Asociación de Economía Digital, en inglés Digital Economy Partnership Agreement ("DEPA") celebrado entre Singapur, Chile y Nueva Zelanda y que entró en vigor a comienzos de 2021. Tanto como con el Acuerdo Transpacífico de Cooperación Económica, en inglés Comprehensive and Progressive Agreement for Trans-Pacific Partnership ("CPTPP"). Las semejanzas casi textuales entre estos sugieren que el Acuerdo tomó el DEPA y el CPTPP como fuentes.

5.1. Convenio N°108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, Estrasburgo, 28.I.1981

El Convenio N°108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, Estrasburgo, 28.I.1981 (en adelante, "Convenio 108") ha sido actualizado por el protocolo de enmienda, conocido como Convenio 108+. A la fecha este último, ha sido firmado por 43 países (incluyendo Argentina) [(134)] y ratificado sólo por 17 (incluyendo a Uruguay) [(135)] de los 55 que son parte del Convenio 108 [(136)].

Al momento de cierre de esta publicación, precisamente el 5 de julio de 2022, la Comisión de Relaciones Exteriores y Culto de la Honorable Cámara de Diputados de la República Argentina le otorgó dictamen favorable al Convenio 108+, dándole paso a la Comisión de Asuntos Constitucionales para su consideración y posterior elevación al recinto en pos de obtener la media sanción.

El Convenio 108 abrió su suscripción en el año 1981 y ha tenido un rol fundamental en la armonización de la legislación en materia de protección de datos personales respecto de sus Estados partes, sirviendo como base para leyes internacionales. El protocolo del 18 de mayo de 2018 conocido como Convenio 108+ buscó modernizar el Convenio 108 y reforzar su aplicación [(137)].

La influencia del Convenio 108 en la región como normativa modelo resulta evidente al revisar su contenido. En primer lugar, requiere que los Estados partes tengan una norma que regule el tratamiento de datos e incorpora principios que se ven replicados en las regulaciones relevadas [(138)].

En este orden, el convenio establece el principio de calidad de los datos, que tal como se refería en apartados anteriores, requiere que los datos tratados, sean proporcionados y apropiados a la finalidad para la cual fueron recolectados. En la versión modernizada del Convenio 108 se agrega bajo el mismo apartado, el principio por el cual la legitimación para el tratamiento de datos personales estará dada por el consentimiento del titular o por una base legítima fundada en ley. Respecto del consentimiento, se indica que éste debe ser libre, específico, informado e inequívoco, todo lo cual hemos encontrado en las normativas de cada uno de los países previamente relevadas [(139)].

La obligación de implementar medidas de seguridad también se introduce como principio bajo el Convenio 108, debiendo garantizar la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizada [(140)]. El Convenio 108+ introduce la obligación de notificación del incidente de seguridad en línea con las tendencias internacionales en la materia [(141)]. Esta obligación de notificación se encuentra expresamente regulada por la normativa en Uruguay [(142)]. En Argentina, hay

quienes sostienen que en base al principio de buena fe y de la Resolución AAIP 47/2018, existiría una obligación de notificar vulneraciones de seguridad.

Respecto de la transferencia internacional de datos, el Convenio 108 busca que los Estados no limiten el flujo transfronterizo de datos arbitrariamente, por lo que la restricción deberá fundarse en la legislación en materia de datos personales. Al respecto, el texto de la versión modernizada resulta más claro en tanto se remite a los niveles adecuados de protección que debe garantizar el receptor de los datos personales cumpliendo como mínimo con el estándar del Convenio 108 [(143)].

Entendemos que el Convenio 108 vigente en Argentina y Uruguay no entraría en contradicción con lo dispuesto en el Acuerdo. Por el contrario, complementa lo allí dispuesto en materia de protección de datos personales. En primer lugar, el Convenio 108 vigente y obligatorio para Argentina y Uruguay resulta una norma específica para estos que debe primar sobre lo dispuesto en el texto de este último. Además, al abordar la protección de datos personales el Acuerdo remite a los estándares internacionales que deberían entenderse por aquellos impuestos por normativa como la del Convenio 108.

5.2. Los Estándares de Protección de Datos de los Estados Iberoamericanos

La Red Iberoamericana de Protección de Datos Personales estableció los Estándares de Protección de Datos de los Estados Iberoamericanos [(144)]. Estos tienen entre sus objetivos establecer un conjunto de principios y derechos comunes en la materia para que los Estados miembros desarrollen legislación homogénea y se garanticen los derechos de las personas físicas dentro del territorio. Al respecto, cabe mencionar que, si bien no son obligatorios, sus preceptos son replicados en algunas de las normativas analizadas bajo este documento e incluso han servido de guía para los procesos de modernización regulatoria como sucede para el caso de Uruguay y Argentina [(145)].

En línea con lo anterior, y siendo que el Acuerdo refiere a que los Estados deberán adoptar regulación que considere los estándares internacionales en la materia, podría entenderse que estos Estándares serán tenido en consideración a los efectos de cumplir con este punto [(146)].

Estos estándares comienzan estableciendo bajo el capítulo I definiciones específicas, tales como, anonimización, consentimiento, datos personales, datos personales sensibles, encargado, exportador, responsable, titular y tratamiento. Además, establece principios generales de protección de datos personales bajo el capítulo II. Tanto las definiciones como los principios se alinean a las de la legislación vigente en los países analizados bajo este documento. Sin embargo, incluyen preceptos que al momento no están receptados en la normativa local, salvo por el caso de Brasil que puede decirse que tiene vigente la norma más moderna de la región. Por ejemplo, los estándares regulan el derecho a la portabilidad, a la impugnación de las decisiones automatizadas, el principio de responsabilidad demostrada, privacidad por diseño y defecto, entre otros que serán analizados a continuación.

5.2.1. Los Principios de Protección de Datos Personales

Los estándares en cuestión reconocen los principios de legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad. Estos se encuentran receptados en la legislación local de los países, salvo respecto de Paraguay que tiene aún pendiente emprender el camino hacia la modernización de su regulación.

El principio de legitimación establece las bases legales del tratamiento de datos, las que incluyen el supuesto de consentimiento del titular, la necesidad del tratamiento para el cumplimiento de una obligación legal o ejecución de un contrato, el interés vital del titular o persona física, el interés público, entre otros [(147)]. El consentimiento se regula específicamente bajo los estándares, tal como sucede en líneas generales con la legislación analizada. Así, se observa que el responsable del tratamiento es quien debe demostrar indubitablemente que el titular ha otorgado el consentimiento mediante una acción afirmativa clara

y que es revocable, para lo cual se deben prever mecanismos sencillos, ágiles, eficaces y gratuitos.

El principio de licitud bajo estos estándares refiere a que el tratamiento de datos debe hacerse en cumplimiento de la ley de cada país.

La lealtad requiere que los datos no sean tratados por medios engañosos o fraudulentos. En este sentido, vemos que este principio se encuentra presente en la normativa del consumidor tanto a nivel regional como en la legislación de cada país [(148)]. En una misma línea se reconoce el principio de transparencia que requiere informar al titular de los datos respecto de su tratamiento [(149)]. En este sentido, se indica que se debe informar acerca de la identidad del responsable, la finalidad del tratamiento, las transferencias internacionales si las hubiera, los derechos que le asisten al titular y el origen de donde hubiera recolectado los datos personales si no fuera directamente del titular. Además, esta información debe ser dispuesta de una forma accesible, en lenguaje sencillo y fácil comprensión para el titular de los datos.

Cabe mencionar que los estándares prevén la excepción de fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público. El principio de proporcionalidad establece que solo pueden ser tratados los datos que sean adecuados, pertinentes y limitados a la finalidad (este también es conocido como de minimización).

El principio de calidad exige al responsable adoptar medidas para mantener los datos exactos, completos y actualizados. Además, en caso de que los datos dejen de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, deben ser suprimidos o anonimizados. En esta línea, se especifica que sólo podrán ser conservados durante el plazo necesario para el cumplimiento de las finalidades que justifican su tratamiento o aquéllas relacionadas con exigencias legales aplicables al responsable. A su vez, respecto de las medidas para garantizar este principio, deben preverse mecanismos y técnicas orientadas a la eliminación definitiva y segura de éstos.

Los estándares receptan el principio de responsabilidad demostrada, que se verifica en la nueva normativa brasileña de protección de datos personales, estableciendo que el responsable deberá implementar medidas para acreditar el cumplimiento de los principios y obligaciones establecidas. La facultad de demostrar el cumplimiento también incluye la capacidad de rendir cuentas sobre el tratamiento al titular y a las autoridades de control. En relación con este punto, se enumeran como ejemplos para cumplir con esta finalidad a las mejores prácticas nacionales, esquemas de autorregulación, sistemas de certificación, entre otros [(150)]. Además, se enumeran mecanismos tendientes a cumplir con este principio, como es el destino de recursos a la instrumentación de programas y políticas de protección de datos personales, la implementación de sistemas de administración de riesgos asociados al tratamiento de datos, programas de capacitación, sistemas de supervisión y vigilancia interna, y procedimientos para recibir requerimientos de titular de datos, entre otros [(151)]. Por último, el principio de responsabilidad también requiere que el responsable revise y evalúe permanentemente los mecanismos que adopte a tales efectos.

La seguridad se reconoce como principio, estableciéndose la necesidad que el responsable del tratamiento cuente con medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales [(152)]. A efectos de determinar las medidas, se establecen los factores que deberán considerarse, tales como el estado de la técnica, los costos de aplicación, alcance, contexto, las finalidades del tratamiento, las transferencias internacionales y las posibles consecuencias de las vulneraciones, entre otros factores [(153)]. Resulta interesante notar que los estándares en cuestión introducen la obligación de notificación del incidente de seguridad al titular y a la autoridad de control, previendo que no sería aplicable en caso de que pudiese demostrarse la improbabilidad de la vulneración y/o que la misma no afecta derechos ni libertades de los titulares involucrados [(154)].

La notificación debe contener cierta información mínima, como la naturaleza del incidente, los datos personales comprometidos, las acciones correctivas, las recomendaciones al titular sobre las medidas que éste puede adoptar para

proteger sus intereses y los medios disponibles para que pueda obtener más información [155]. En lo que respecta al responsable, éste deberá documentar todo lo relativo a la vulneración de seguridad de los datos personales ocurrida, como la fecha, el motivo, los hechos relacionados y las medidas correctivas adoptadas.

La obligación de guardar confidencialidad de los datos personales tratados se reconoce como principio que debe extenderse a todos los que intervengan en ese tratamiento. La obligación de confidencialidad subsistirá aún cuando se finaliza la relación con el titular del dato [156].

5.2.2. Derechos de los y las titulares de datos personales

El documento reconoce los derechos ARCO del titular de los datos personales bajo el Capítulo III. Estos son el derecho de acceso, rectificación, cancelación y oposición [157]. Además, reconoce el derecho a la portabilidad [158], a no ser objeto de decisiones individuales automatizadas [159] y a limitar el tratamiento de los datos personales [160]. Estos derechos no son excluyentes, es decir que el ejercicio de uno no obsta el ejercicio de otro [161].

El derecho de acceso se refiere a la facultad del titular de conocer los datos que estén en posesión del responsable del tratamiento, así como toda la información relativa a las condiciones generales y específicas de su tratamiento [162].

El derecho de rectificación está dado por la facultad del titular de solicitar que se rectifiquen o corrijan sus datos personales cuando estos resulten inexactos, incompletos o no se encuentren actualizados [163].

La facultad del titular de solicitar la cancelación o supresión del dato se encuentra regulada bajo el punto 27 de los estándares e implica que los datos en cuestión dejen de estar en posesión del responsable y de ser tratados por éste [164].

La facultad de oponerse a un tratamiento se encuentra regulada específicamente estableciéndose que los supuestos en los que se podrá

solicitar serán cuando: (i) exista una razón legítima o (ii) el tratamiento tenga por fin la mercadotecnia directa (incluyendo la elaboración de perfiles) [(165)].

El derecho a no ser objeto de decisiones automatizadas, en los tiempos actuales del desarrollo del big data y la inteligencia artificial, es sin duda relevante y se alinea con la normativa europea en la materia. Al reconocer este derecho, los estándares limitan aquellas decisiones automatizadas -sin intervención humana- que produzcan efectos jurídicos o afecten de manera significativa al titular y que tengan por fin evaluar, analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

En relación con las decisiones automatizadas, es relevante destacar que el documento de los estándares es del 2017 y que, a la fecha, vemos que el avance de la tecnología y la automatización de los procesos ha evolucionado de forma considerable. Un ejemplo interesante es el otorgamiento de créditos personales que efectúan algunos bancos digitales o fintech de la región que, con la mira puesta en la inclusión financiera para ampliar su cartera de clientes, implementan mecanismos no tradicionales que implican el entrecruzamiento y tratamiento intensivo de datos personales [(166)]. Estos mecanismos utilizan datos obtenidos del sistema financiero tradicional -cuando existen- y datos relativos al comportamiento en redes sociales, entre otras "huellas digitales" que dejan los usuarios y usuarias al navegar por internet y resultan relevantes para determinar la capacidad de pago de la persona. De esta forma, al combinar la información con algoritmos las empresas logran un perfilamiento y un scoring crediticio enriquecido. Este les permite calcular de forma automatizada la tasa de repago y, de esa forma, determinar el monto, plazo y tasa de interés a ser ofrecida al usuario/a de forma personalizada.

Si bien estos mecanismos pueden ser positivos para la inclusión financiera, siendo uno de los objetivos más importantes de los países de la región, cabe preguntarse si estas técnicas de segmentación, perfilamiento y scoring automatizado intensivas resultan acordes a los estándares bajo análisis. En esta clase de ejemplos aparecen interrogantes similares a los relacionados con el

tratamiento intensivo con fines de publicidad, tanto en cuanto a la cuestión del consentimiento, como al derecho a no ser objeto de decisiones automatizadas.

El desafío está planteado, considerando, por un lado, la importancia del desarrollo tecnológico para poder brindar más y mejores servicios a la población de la región, sin poner trabas a la innovación de las pymes y el fomento de la economía del conocimiento. Y, por el otro lado, manteniendo los más elevados estándares de seguridad, protección de datos personales, lealtad comercial, no discriminación y, en definitiva, de respeto por la dignidad y los derechos humanos de los usuarios [(167)].

En relación con la cuestión de las decisiones automatizadas, los estándares flexibilizan el criterio y se indica que no resultará aplicable cuando "... el tratamiento automatizado de datos personales sea necesario para la celebración o la ejecución de un contrato entre el titular y el responsable; esté autorizado por el derecho interno de los Estados Iberoamericanos, o bien, se base en el consentimiento demostrable del titular" [(168)]. Volviendo al ejemplo introducido con anterioridad, un banco podría válidamente conceder un crédito en base a una decisión automatizada si cuenta con el consentimiento del titular del dato para tal tratamiento. Sin perjuicio de lo anterior, los estándares establecen que cuando la decisión automatizada esté permitida en base a un consentimiento o relación contractual, el titular siempre tendrá derecho a obtener la intervención humana, recibir una explicación sobre la decisión tomada, expresar su punto de vista e impugnar la decisión [(169)].

Los estándares receptan los lineamientos de los derechos humanos, incluyendo prohibiciones expresas respecto a decisiones automatizadas cuando estas tengan efectos discriminatorios: "El responsable no podrá llevar a cabo tratamientos automatizados de datos personales que tengan como efecto la discriminación de los titulares por su origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, así como datos genéticos o datos biométricos" [(170)].

El derecho a la portabilidad, reconocido en normativas como la europea, se recepta en estos estándares a los efectos de otorgar al titular la potestad de obtener una copia de los datos personales que sean objeto de tratamiento. Los datos deben ser entregados en un formato estructurado de lectura común que permita seguir utilizándolos o transferirlos a otro responsable (171). El ejercicio de este derecho presenta un desafío para los responsables del tratamiento ya que la tecnología suele no ser neutral ni interoperable, en el sentido que no se utiliza el mismo formato de datos y estructuración a un sistema común o neutral y en ocasiones puede ser excesivamente costoso o de imposible cumplimiento. Quizás en este entendimiento los estándares refieren a que cuando sea técnicamente posible el titular podrá requerir la transferencia de sus datos a otro responsable (172).

La portabilidad no alcanza a los datos que sean "...información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular..." (173). Seguidamente, se aclara a modo ilustrativo que no alcanzaría a aquellos datos que sean el resultado de haber sometido los datos personales a un proceso de personalización, recomendación, categorización o creación de perfiles. Esto tiene sentido, por cuanto ese tipo de tratamientos responde en general a la utilización de técnicas confidenciales o algoritmos de procesamiento propias del know how del responsable o de sus proveedores de servicios.

El derecho a la limitación del tratamiento refiere a que al momento de remitir un requerimiento de rectificación u oposición el responsable deberá limitar el tratamiento al simple almacenamiento, hasta tanto se resuelva (174). Asimismo, el titular podrá requerir esta limitación cuando el tratamiento no sea necesario para el responsable, pero necesite que los datos sigan siendo almacenados por él, con el objeto de formular una reclamación relativa a estos.

A los efectos de garantizar el ejercicio de los derechos reconocidos, los estándares precisan que los responsables implementen procedimientos para su ejercicio mientras que los requerimientos, plazos, términos y condiciones del ejercicio serán determinados por cada Estado. En cuanto

a esto último, los estándares requieren a los Estados que determinen las causales de improcedencia de los derechos, que podrían estar relacionadas al cumplimiento de sus funciones o al tratamiento necesario para el cumplimiento de una obligación legal, entre otros supuestos [(175)].

Si bien el derecho a la protección de datos personales suele vincularse como derecho derivado del derecho personalísimo a la privacidad, bajo los estándares se admite el ejercicio de estos derechos por parte de personas vinculadas a una persona fallecida [(176)]. Este punto resulta novedoso en tanto las regulaciones analizadas bajo este artículo no suelen resolver esta cuestión [(177)].

Por último, el documento exige a los Estados reconocer al titular la posibilidad de impugnar las respuestas de los responsables ante sus requerimientos, tanto ante este como ante la autoridad de control y en su caso ante instancias judiciales.

5.2.3. Transferencias internacionales de datos personales

Los estándares dedican un capítulo a la regulación en materia de transferencias internacionales de datos personales indicando los supuestos en que se admiten. En línea con las regulaciones que se abordaron en este documento, se establece que podrán transferirse cuando el país de destino otorgue niveles adecuados de protección de datos personales, se suscriban cláusulas contractuales o cualquier otro instrumento que ofrezcan garantías suficientes. Asimismo, que existen mecanismo de autorregulación vinculante o mecanismos de certificación entre el exportador y el destinatario que sea acorde a la legislación vigente en los Estados o si la autoridad de control autoriza tal transferencia [(178)].

Los estándares otorgan la facultad a los Estados de establecer límites a las transferencias internacionales por categorías de datos, razones de seguridad nacional o pública, protección de la salud pública, derechos y libertades de terceros, u otras cuestiones de interés público [(179)].

En lo que respecta a este punto, cabe mencionar que en noviembre de 2021 la Red Iberoamericana de Protección de Datos Personales abrió a consulta una guía de su elaboración para el uso de las cláusulas contractuales como alternativa para realizar transferencias internacionales de datos personales. Esta guía incluye cláusulas con modelos de adopción para transferencias internacionales entre responsables y entre responsables (controllers) y encargados (processors) para garantizar un mínimo de protección entre los Estados. Entendemos que, en caso de aprobarse, serviría para armonizar los marcos normativos de transferencias internacionales de datos personales entre los Estados, alineados con un alto estándar de protección de los derechos de los titulares de los datos personales.

5.2.4. Privacidad por diseño y por defecto

Los estándares interpelan a los Estados a adoptar medidas proactivas que promuevan el cumplimiento de su legislación y eleven los controles implementados por el responsable [(180)]. A tales efectos, se introduce el concepto de privacidad por diseño y por defecto [(181)]. Esto último refiere a que el responsable debe contemplar la privacidad de los datos y el cumplimiento de la normativa desde el diseño, es decir desde que se determina el tratamiento, y este principio debe regir durante el mismo. A su vez se refiere a que la tecnología y los procesos deben contemplar la privacidad por defecto y se debe ajustar a los principios, derechos y normativa aplicable.

Si bien la privacidad por diseño y por defecto no se encuentra expresamente como principio en la normativa analizada bajo este documento, existe un avance en este sentido en los proyectos de reforma de la región y en los diferentes lineamientos que emitan las autoridades de control de los países. A modo de ejemplo, las autoridades de Argentina y Uruguay emitieron un guía de Evaluación de Impacto en la Protección de Datos que expresamente incorpora estos principios [(182)] y en el caso de Uruguay se enumera la privacidad por defecto y diseño comprendidas dentro del ejercicio de la responsabilidad proactiva que deben tomar los responsables del tratamiento.

5.2.5. Oficial de cumplimiento

La designación de un oficial de cumplimiento es una buena práctica que receptan los estándares. Este requerimiento no es para todo tipo de responsables sino que se establecen los supuestos en los que sería aplicable. Por ejemplo, cuando el responsable sea el Estado, o cuando el tratamiento de datos personales tenga por objeto una observación habitual y sistemática de la conducta del titular, o cuando el tratamiento entrañe un riesgo alto para los titulares de los datos [(183)].

5.2.6. Mecanismos de autorregulación

La autorregulación y el principio de lo que se conoce como responsabilidad demostrada prima a lo largo del texto y en las últimas tendencias en materia regulatoria [(184)]. En lo que respecta puntualmente a los estándares, bajo el punto 40 se indica que los responsables podrán adherir a este tipo de mecanismos de autorregulación, que incluso podrán comprender procedimientos de resolución de conflictos [(185)]. Esto último es sin dudas una novedad, siendo que las normativas analizadas entienden la regulación en la materia como de orden público y en principio no habilitan este tipo de soluciones alternativas autorreguladas de conflicto.

Expresamente, los estándares refieren a los códigos deontológicos y sistemas de certificación y sus respectivos sellos de confianza como mecanismos de autorregulación que contribuyen al cumplimiento y aplicación del régimen de datos [(186)]. Cabe mencionar que la legislación nacional de cada uno de los Estados, aplicable en la materia, deberá establecer las reglas para la validación, confirmación o reconocimiento de estos mecanismos de autorregulación [(187)].

5.2.7. Evaluación de impacto

La evaluación de impacto es una buena práctica [(188)] que muchas regulaciones, como la europea, han recogido como obligatoria. En este caso, los estándares las prevén para aquellos tratamientos de datos personales que entrañan un

alto riesgo para los derechos de los titulares. Son los Estados quienes deberán determinar los casos específicos en los que serán obligatorias y el contenido de las mismas, entre otras cuestiones [(189)]. En lo que respecta a la región, y sin perjuicio de que en Argentina y Uruguay se recomiendan como buena práctica, por el momento sólo la normativa de Brasil incorpora las evaluaciones de impacto expresamente [(190)].

5.3. Acuerdo de Asociación de Economía Digital, en inglés Digital Economy Partnership Agreement ("DEPA") de Chile, Nueva Zelanda y Singapur.

El DEPA es un acuerdo recientemente celebrado entre Chile, Nueva Zelanda y Singapur [(191)]. Se trata de un acuerdo novedoso, focalizado en fortalecer la cooperación en cuestiones emergentes claves de la economía digital, y en promover la interoperabilidad entre los sistemas de los países miembros. Destacamos que es un tratado relacionado con el Acuerdo Transpacífico de Cooperación Económica, en inglés Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) dado que los tres países, Singapur, Chile y Nueva Zelanda, son miembros del CPTPP, y en cierta forma el DEPA lo complementa, profundizando las obligaciones en el ámbito digital. Además, es un acuerdo abierto a otros miembros de la Organización Mundial de Comercio (OMC). Por el momento, únicamente Canadá mostró interés formal en unirse y dio inicio a las discusiones con los restantes países miembros a tal efecto [(192)].

El DEPA trata aspectos tales como facilitar el comercio digital punto-a-punto, a través del reconocimiento de las identidades digitales, la facturación electrónica, el comercio sin documentos físicos (paperless) y la cooperación en soluciones de fintech y pagos electrónicos. Además, trata aspectos como permitir el flujo de datos de confianza mediante mecanismos de protección de datos personales, transferencias internacionales de datos, datos de gobierno abierto e innovación en datos y regulación; construir la confianza en sistemas digitales y facilitar las oportunidades de participación en la economía digital, a través de la adopción de un marco ético de inteligencia artificial, la protección

del consumidor en línea, la cooperación entre pequeñas y medianas empresas, y la promoción de la inclusión y participación digital [(193)].

Es interesante notar que el DEPA y el Acuerdo del Mercosur tienen objetivos y estructuras similares: ambos reconocen la importancia del comercio electrónico y de la economía digital para el desarrollo de sus respectivos países y tratan diversos aspectos regulatorios con impacto en los intercambios electrónicos. Sin embargo, el enfoque que adopta el DEPA es en algunos puntos diferente al del Acuerdo del Mercosur. Por ejemplo, el primero establece obligaciones más detalladas y específicas, lo que resulta en un acuerdo más extenso y preciso, mientras que el segundo establece obligaciones y estándares generales. Mientras que el Acuerdo del Mercosur indica de forma general que "cada parte procurará adoptar medidas para facilitar el comercio realizado por medios electrónicos" (art. 2.6), el DEPA prevé un módulo entero sobre este punto (Módulo 2), donde se refiere a la comercialización paperless, a la logística del comercio cross-border, a la facturación electrónica, a los envíos express y a los pagos electrónicos. Asimismo, más adelante en su texto, el DEPA se pronuncia sobre datos abiertos, ética en la inteligencia artificial y cooperación de pequeñas y medianas empresas, entre otros aspectos, sobre los cuales el Acuerdo del Mercosur no se explaya [(194)]. Por último, el DEPA establece un sistema específico de solución de controversias; que no se trata en el Acuerdo del Mercosur, quizás por el contexto de cooperación regional y los mecanismos preexistentes entre los Estados parte sobre este punto.

De todos modos, los textos son llamativamente similares en muchos aspectos, incluido en lo referido a la protección de datos personales. En el Anexo I analizamos los textos cercanos en detalle, y a continuación proveemos un resumen:

- Definición de datos personales: Ambos acuerdos se refieren a la información o datos personales como información respecto de una persona física identificada o identificable [(195)].
- Beneficios de la protección de datos: Ambos reconocen los beneficios de proteger la información personal y su impacto en mejorar la confianza en el comercio digital [(196)].

- Marco legal de la protección de información personal y principios internacionales: Ambos establecen que cada parte adoptará o mantendrá normas que protejan la información personal de los usuarios y las usuarias del comercio electrónico. A tal fin, el DEPA indica tomar en consideración los "principios y directrices de los organismos internacionales pertinentes", mientras que el Acuerdo apunta a los "estándares internacionales que existen en esta materia". El Acuerdo lista algunos principios específicos ("previo consentimiento, finalidad, calidad, seguridad, responsabilidad, entre otros.") y el DEPA se refiere a otros ("(a) limitación de recolección; (b) calidad de datos; (c) especificación de propósito; (d) limitación de uso; (e) salvaguardias de seguridad; (f) transparencia; (g) participación individual; y (h) rendición de cuentas."). El DEPA además menciona que el marco normativo se compondrá no solo de las leyes que abarquen de manera amplia la privacidad, sino también de las sectoriales específicas sobre protección de datos y las que dispongan la aplicación de compromisos voluntarios de empresas relacionados con la protección de datos personales o la privacidad [(197)].
- Aplicación no discriminatoria: El DEPA habla de la aplicación no discriminatoria de la normativa de protección a los usuarios, mientras que el Acuerdo se refiere a la aplicación no discriminatoria del marco legal doméstico de protección de la información personal [(198)].
- Publicación de información sobre la protección de la información personal: Los textos son virtualmente idénticos; ambos establecen que las partes deben proveer información tanto para que los individuos puedan ejercer sus derechos, como para que las empresas puedan cumplir con la normativa [(199)].
- Intercambio de información y experiencias en materia de protección de datos: Ambos prevén el intercambio de información en la materia. El DEPA agrega que este se orienta a promover la compatibilidad e interoperabilidad entre las partes [(200)].
- Transferencia transfronteriza de información por medios electrónicos: Ambos textos indican que las partes reconocen que cada una podrá tener sus requisitos regulatorios y permiten la transferencia transfronteriza de información para la realización de la actividad comercial. Esto se

efectúa con la salvedad de que se permite a las partes adoptar medidas específicas en contrario para alcanzar un objetivo de política pública, siempre que no medie discriminación arbitraria ni exista una restricción encubierta al comercio [(201)]. El texto del DEPA agrega que, en este último caso, la medida no impondrá restricciones a las transferencias de información mayores a las que se requieren para alcanzar el objetivo. El Acuerdo del Mercosur, por su lado, indica que el artículo no se aplica a los servicios financieros.

También se prevén puntos que, aunque no se tratan directamente sobre la protección de datos personales, están relacionados:

- Ubicación de las instalaciones informáticas: Ambos textos también son prácticamente idénticos, estableciendo que una parte no podrá exigir a la otra usar o ubicar las instalaciones informáticas en su territorio e incluye salvedades por objetivos de política pública, similares a las del artículo anterior [(202)]. El Acuerdo del Mercosur también indica que el artículo no se aplica a los servicios financieros.
- Protección al consumidor en línea: Los textos comienzan de forma muy similar, destacando la importancia de la protección al consumidor en el comercio electrónico [(203)]. Sin embargo, mientras que el Acuerdo hace referencia a la normativa específica del Mercosur sobre la protección del consumidor [(204)]; el DEPA dedica un capítulo especial a medidas puntuales, incluyendo explorar los beneficios de mecanismos de solución de controversias alternativos.
- Principios sobre el acceso y el uso del internet: Ambos textos reconocen los beneficios de que los consumidores puedan acceder y usar los servicios y aplicaciones disponibles en internet, conectar los dispositivos de su elección y acceder a información sobre prácticas de redes [(205)].
- Además, se prevén otros puntos similares, ya no con el mismo texto pero con similares conceptos y medidas a tomar:
- Mecanismos de seguridad: El Acuerdo menciona que las partes fomentarán la utilización de mecanismos de seguridad y la disociación o anonimización de datos. El DEPA, por su parte, dedica un capítulo más específico a la ciberseguridad [(206)]. Ambos textos reconocen expresamente

la importancia de la cooperación en materia de ciberseguridad [207].

- Autorregulación, Contratos y sellos de confianza: El Acuerdo indica que las partes admitirán para el sector privado la implementación de contratos o autorregulación para aplicar a los datos personales un nivel de protección adecuado [208]. El DEPA, por su parte, indica que las partes alentarán (y no sólo admitirán) la adopción por parte de las empresas de sellos de confianza que ayuden a verificar su conformidad con estándares de protección de datos personales y con mejores prácticas. Además, intercambiarán información y compartirán experiencias sobre su uso; y procurarán reconocer mutuamente los sellos de confianza de protección de datos de las otras partes como mecanismos válidos para facilitar las transferencias transfronterizas de información [209].
- Si bien el Acuerdo menciona los sellos de confianza, lo hace en el marco de las disposiciones generales para promover la confianza y la seguridad jurídica en el comercio electrónico (art. 2.5.b), junto con las directrices, modelos de contratos y códigos de conducta. El Acuerdo habla de la autorregulación (no necesariamente mediante sellos) y sólo las menciona en el marco de la transferencia internacional de datos, pero no para cualquier aspecto de la protección de datos.
- Comunicaciones comerciales directas no solicitadas: El Acuerdo busca proteger de manera efectiva a los usuarios finales contra las comunicaciones comerciales directas no solicitadas. Para ello, solicita consentimiento previo que será "definido conforme a las leyes y disposiciones de cada parte", permitiendo las comunicaciones comerciales directas en el marco de una venta de un producto o servicio, en línea con el texto del posible acuerdo del Mercosur y Unión Europea [210]. El DEPA, en cambio, también prevé un capítulo especial sobre este punto pero es más estricto al respecto, agregando incluso un punto sobre la minimización de los mensajes no solicitados [211].

Como conclusión de esta subsección es interesante notar la cercanía de ambos documentos no sólo en sus textos sino también en la fecha de firma (el DEPA celebrado en 2020 y el Acuerdo del Mercosur en abril de 2021). Quizás el momento de celebración del Acuerdo tenga que ver con el freno

a las negociaciones para un tratado de libre comercio entre Singapur y el Mercosur, que algunas fuentes indican que ocurrió a mediados de 2020 debido a la pandemia [212]. Sin embargo, es conveniente completar el análisis con las similitudes con el CPTPP, que veremos a continuación.

5.4. Acuerdo Transpacífico de Cooperación Económica, en inglés Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)

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) [213], que no prosperó luego de que Estados Unidos se retirara de su negociación.

El CPTPP incorpora el texto del TPP por referencia y su Capítulo 14 es específico sobre comercio electrónico [214]. Este contiene disposiciones sobre protección de datos personales y otros aspectos del comercio electrónico.

Destacamos los siguientes puntos comparativos en relación con el Acuerdo e incluimos en el Anexo 1 la comparación de los textos pertinentes:

- Derechos aduaneros: El artículo 14.3 del CPTPP es sustancialmente similar al artículo 3 del Acuerdo. Ambos textos impiden aplicar derechos aduaneros a las transmisiones electrónicas cross-border. Sin embargo, ambos permiten la aplicación de impuestos internos, tarifas o cargas que sean compatibles con acuerdos comerciales internacionales (de la OMC en el caso del Acuerdo y del mismo CPTPP en su caso).
- Autenticación electrónica: Los textos del artículo 14.6 del CPTPP y del artículo 4 del Acuerdo son casi idénticos. Ambos impulsan el reconocimiento de firmas digitales o electrónicas de otras jurisdicciones y se comprometen a fomentar la interoperabilidad en este ámbito.
- Protección al consumidor en línea: El artículo 5 del Acuerdo protege

específicamente al consumidor en línea, con lenguaje similar a como lo hace el artículo 14.7 del CPTPP. Mientras que este último incluye previsiones específicas, el Acuerdo llama a la normativa del MERCOSUR al respecto.

- Cooperación: El artículo 12 del Acuerdo, de forma similar al artículo 14.15 del CPTPP, prevé la cooperación en regulaciones en la esfera del comercio electrónico y, de forma interesante, indica en una copia casi textual del CPTPP que se fomentará "el desarrollo por parte del sector privado de los métodos de autorregulación que fomenten el comercio electrónico, incluyendo códigos de conducta, contratos modelo, directrices y mecanismos de cumplimiento". En relación a la referencia del texto a la autorregulación cabe puntualizar que entendemos que el texto del CPTPP -en línea con el del Acuerdo- aspira a un marco de co-regulación en el que coexistan la regulación estatal y aquellos mecanismos desarrollados por privados para fomentar la capacitación, y lograr un mayor cumplimiento y adhesión a la regulación vigente. Tanto el CPTPP como el Acuerdo introducen regulación pero delimitan un espacio para el desarrollo de la autorregulación por parte de privados reconociendo en cierto punto su utilidad para llenar los vacíos entre la regulación y la implementación y operatividad de la norma.

Vemos entonces que los Artículos 3, 4, 5, 6, 8, 9, 11 y 12 del Acuerdo del Mercosur encuentran su fuente directa en artículos equivalentes del CPTPP, y que muchos de ellos sirvieron a su vez como fuente del DEPA y de los acuerdos de libre comercio entre Argentina y Chile, y Uruguay y Chile. Es interesante señalar entonces que el Acuerdo está en gran medida sujeto a las mismas críticas que recibieron estos tratados (especialmente el TPP y el CPTPP) respecto de la protección de datos, especialmente en lo referido a los tibios compromisos asumidos.

6. Conclusiones: Oportunidades y desafíos para la protección de datos personales y el desarrollo del comercio electrónico en el Mercosur

Como conclusión del presente trabajo destacamos tres aristas de análisis de oportunidades y desafíos para la protección de datos personales y el desarrollo del comercio electrónico en el Mercosur:

6.1. El impacto del Acuerdo en las legislaciones nacionales de los Estados parte: Argentina, Paraguay y Uruguay deberán adaptar su legislación local de protección de datos personales

En primer lugar, el Acuerdo brinda un marco general para las legislaciones nacionales de protección de datos de cada uno de los países del Mercosur: Argentina, Brasil, Paraguay y Uruguay. En general, vemos que las disposiciones del Acuerdo sobre estándares internacionales y principios generales respecto a la protección de datos personales responden a la tendencia normativa en la materia. De esta forma, el Acuerdo es, en cierta medida, útil a los fines de armonizar e impulsar la modernización de legislación en la materia, que se está dando de forma dispar en la región, siendo Brasil el país que lleva la delantera. La celebración del Acuerdo en sí es un acto importante para el bloque del MERCOSUR, un signo de la voluntad de los Estados miembro de acompañar al desarrollo sostenido del comercio electrónico y de hacerlo de forma respetuosa de la protección de los derechos de los consumidores y de sus datos personales. Sin embargo, el Acuerdo resulta un tanto débil para mejorar el respeto por la protección de datos personales en la región.

Respecto de cada Estado parte en particular, vemos que la normativa en materia de protección de datos personales vigente en Argentina y Uruguay se alinea a los estándares del Acuerdo, por lo que en caso de entrar en vigor el

Acuerdo, el impacto en este aspecto no debería ser significativo. Sin perjuicio de lo anterior, tanto Argentina como Uruguay y Paraguay deberán adecuar la normativa que regula el envío de comunicaciones comerciales no solicitadas a los fines de marketing (art. 10 del Acuerdo, que se inspira en el art. 48 del texto negociado del acuerdo Mercosur - Unión Europea). En relación con este punto, deberá receptarse expresamente que, en principio, estas comunicaciones se encuentran prohibidas y que el único supuesto que las habilita es aquel que se da en el contexto de una relación previa ("venta de un producto o servicio") con el usuario o consumidor y siempre que la comunicación esté relacionada con productos o servicios similares.

En lo que respecta a Paraguay, el desafío de alcanzar el estándar propuesto por el Acuerdo en materia de protección de datos personales será mayor que para el resto de los países. Esta jurisdicción deberá rediseñar el esquema normativo a fin de alinearlo a los estándares internacionales y regular el tratamiento de los datos personales desde una perspectiva integral (no sólo aquellos vinculados a los datos crediticios), incluyendo de forma expresa principios tales como el de finalidad y responsabilidad, y las transferencias internacionales de datos, entre otros puntos. Sobre Brasil, se advierte que la entrada en vigor no tendrá mayor impacto en la legislación, siendo que su normativa actual es de las más modernas de la región y se encuentra plenamente alineada a los dispuesto en el Acuerdo.

Es interesante notar que efectivamente la convergencia regulatoria en los países del Mercosur se ve impulsada por un tratado de libre comercio [(215)].

6.2. La similitud del texto del Acuerdo con otros convenios internacionales de comercio muestra su valor para que el Mercosur retome negociaciones internacionales con la Unión Europea y con los países del CPTPP

En segundo lugar, el Acuerdo es ciertamente similar a otros acuerdos comerciales internacionales, tales como los textos del DEPA, del CPTPP y de los

acuerdos de libre comercio entre Argentina y Chile, y Uruguay y Chile. Si bien los textos son acordes a las legislaciones locales y a otros que aplican a todos o a algunos de los Estados parte (tales como el Convenio 108 y los Estándares Iberoamérica), cabe preguntarse: ¿por qué el Mercosur celebra este Acuerdo ? ¿Por qué elige este texto y por qué lo hace ahora? Una posible explicación es la intención del Mercosur de insertarse en el comercio electrónico internacional con la Unión Europea y los países de la costa del Pacífico, especialmente luego de que las negociaciones de ciertos acuerdos comerciales (por ejemplo, con la Unión Europea y con Singapur) se frenaran tan solo unos meses antes de la pandemia del Covid-19. Son miembros del CPTPP Chile, México, y Perú (aunque actualmente el CPTPP sólo se encuentra vigente respecto de México y Perú, no aún de Chile) y es probable, que los miembros del Mercosur estuvieran interesados en seguir los pasos de estos países para fortalecer el comercio internacional, especialmente una vez vigentes los acuerdos del libre comercio Argentina y Chile, y Uruguay y Chile.

Respecto del CPTPP y del DEPA, fuente principal del Acuerdo del Mercosur, lo cierto es que ambos son tratados muy recientes y en la práctica está por verse cómo impactará en el bloque el tomar esta normativa foránea. Vemos que el Acuerdo del Mercosur es algo más limitado y escueto que los otros textos. El Acuerdo parece ser, en algún punto, una adopción modesta de la normativa internacional, que pretende establecer estándares similares y "hablar el mismo idioma" que los países del Pacífico, pero sin realizar cambios radicales en las legislaciones locales de cada uno de los Estados parte [(216)].

El riesgo para el Mercosur con la adopción de textos tan similares al CPTPP y al DEPA, es estar sujeto a las mismas críticas que éstos sufrieron: que se trata de acuerdos con compromisos demasiado laxos que consolidarán el dominio del mercado de las grandes empresas de tecnología al tiempo que limitarán la capacidad de los gobiernos para abordar una serie de desafíos regulatorios, que tampoco logra cerrar la brecha comercial digital entre los países desarrollados y en desarrollo, y que ofrece sólo promesas débiles de diálogo sobre los temas de las pequeñas y medianas empresas (pymes), los pueblos indígenas, los grupos vulnerados, las mujeres y las comunidades marginadas [(217)]. Se trata de

acuerdos que, si bien incluyen temas importantes, pueden ser criticados por ser su regulación específica demasiado moderada, constituyendo una oportunidad perdida para establecer compromisos más concretos junto con mínimos sustantivos de respeto a la protección de datos personales y a la privacidad, como derechos humanos fundamentales.

6.3. La promoción del comercio electrónico y de la co-regulación puede ser positiva para la protección de los datos personales, la privacidad y los derechos humanos en la región

En tercer lugar, respecto del desarrollo del comercio electrónico respetuoso de la protección de los datos personales, la privacidad y los derechos humanos, destacamos que el Acuerdo sienta bases interesantes para promover el desarrollo de la economía digital y del comercio electrónico en la región. Sin embargo, este desarrollo se ve afectado por otros factores que tienen una incidencia directa que es conveniente tener en cuenta, pero que exceden el alcance de este trabajo (como sucede, por ejemplo con los regímenes tributarios y aduaneros, entre otros). No obstante, entendemos que el camino hacia la armonización normativa del comercio electrónico y de la protección de datos en que se inserta el Acuerdo ayudará al desarrollo de una economía digital saludable y pujante dentro de la región.

Por último, y considerando que el Acuerdo menciona el fomento de los métodos de autorregulación y que dicho concepto se analiza de forma cautelosa en el contexto de los derechos humanos, entendemos que su inclusión resulta apropiada por tratarse de mecanismos que complementan la normativa vigente y los mecanismos de enforcement jurisdiccionales, fomentando en los hechos un esquema de co-regulación en lo referido específicamente al comercio electrónico y la protección de datos personales. Tal como hemos reseñado en la sección de los antecedentes, nos encontramos con una región cuyo motor de crecimiento son las pymes, las cuales se fueron volcando al canal online año tras año, de forma constante pero mucho más

lenta que en los países más desarrollados. Con la pandemia del Covid-19, este proceso se vio acelerado de forma abrumadora, lo que llevó incluso a la región a ser considerada la de más rápido crecimiento del mundo. Este contexto implica una carrera también acelerada por la profesionalización y la capacitación de los recursos humanos, considerando que la oferta (empresas que venden productos y servicios online) necesita ponerse al día para cumplir con la regulación, así como con los estándares comerciales, técnicos y legales de la industria, y así poder gestionar de forma exitosa y respetuosa sus actividades de comercio electrónico.

Siguiendo lo anterior, entendemos que las herramientas de autorregulación (como pueden ser los sellos de confianza y los códigos de conducta asociados a ellos) en conjunto y como complemento de la regulación del Estado facilitan a las pymes una hoja de ruta simplificada para la comprensión y el cumplimiento de la normativa aplicable, los estándares de seguridad y transparencia, y las mejores prácticas de la industria. Al mismo tiempo que fomentan la confianza en los/as consumidores/as, tan necesaria en el contexto transfronterizo.

Así, diversos esquemas de co-regulación brindan soluciones que se destacan por el énfasis puesto en materia de derechos de los consumidores y protección de datos personales, y funcionan como mecanismos de capacitación, difusión y concientización para que se logre la operatividad e implementación de las mejores prácticas. Todo eso impacta positivamente en los actores de la región involucrados, tanto públicos como privados, y en beneficio del respeto de los derechos de las personas consumidoras y usuarias de la región, siempre considerando a estos mecanismos como un complemento de la normativa y de los mecanismos de enforcement jurisdiccionales, pero nunca como un reemplazo.

No podemos dejar de mencionar el ejemplo del Distintivo Digital de Profeco reseñado anteriormente como un esquema de co-regulación exitoso.

Por último, el fomento de estos esquemas de co-regulación en los que se incluyen mecanismos como sellos de confianza y códigos de conducta no sólo

es acertado, sino que se debería fomentar y profundizar en nuestra región por su capacidad para lograr adherencia y operatividad a la normativa vigente. Todo ello de forma tal que permita aprovechar su potencial por medio de proyectos público-privados que apunten a abordar temáticas tales como la transferencia internacional de datos, la protección de los usuarios y las usuarias ante el uso intensivo de nuevas tecnologías de perfilamiento en la industria de la publicidad y el marketing digital, la protección de las poblaciones vulneradas en el marco de la economía digital, entre muchos otros.

7. Anexo: Comparación entre textos similares del Acuerdo del Mercosur, el DEPA y el CPTPP

Los artículos 3, 4, 5, 6, 8, 9, 10, 11 y 12 del Acuerdo del Mercosur encuentran su fuente directa en artículos equivalentes del CPTPP.

Los artículos 5, 6, 7, 8, 9, 10 y 11 del Acuerdo del Mercosur encuentran su fuente directa en artículos equivalentes del DEPA (que en algunos casos, como los artículos 6 y 9, éste también se inspira en el CPTPP). Los artículos 2 y 12 del Acuerdo, si bien no son tan similares en su redacción, contienen preceptos relacionados al DEPA.

	Acuerdo del Mercosur	DEPA	CPTPP
Derechos aduaneros	Art. 3: "1. Ninguna Parte impondrá derechos aduaneros a las transmisiones electrónicas entre una persona de una Parte y una persona de otra Parte. 2. Para mayor certeza, el párrafo 1 no impedirá que una Parte imponga impuestos internos, tarifas u otras cargas sobre las transmisiones electrónicas, siempre que dichos impuestos, tarifas o cargas se impongan de una manera compatible con los Acuerdos de la Organización Mundial de Comercio (OMC)".	-	Art. 14.3: "1. Ninguna Parte podrá aplicar derechos aduaneros a las transmisiones electrónicas, incluyendo el contenido transmitido electrónicamente, entre una persona de una Parte y una persona de otra Parte. 2. Para mayor certeza, nada en el párrafo 1 impedirá que una Parte imponga impuestos internos, tarifas u otras cargas sobre el contenido transmitido electrónicamente, siempre que dichos impuestos, tarifas o cargas se impongan de una manera que sea compatible con el presente Acuerdo."

Autenticación	Art. 4: "1. Una Parte no negará la validez legal de una firma únicamente sobre la base de que ésta sea realizada por medios electrónicos, salvo disposición expresa en contrario prevista en su respectivo ordenamiento jurídico. 2. Ninguna Parte adoptará o mantendrá medidas sobre autenticación electrónica que: (a) prohíban a las partes en una transacción electrónica el determinar mutuamente los métodos de autenticación adecuados para esa transacción; o (b) impidan a las partes de una transacción electrónica tener la oportunidad de probar ante las instancias judiciales o administrativas que su transacción cumple con algún requerimiento legal de autenticación. 3. Sin perjuicio de lo dispuesto en el párrafo 2, una Parte podrá requerir, para una categoría determinada de transacciones, que el método de autenticación cumpla con ciertos estándares de desempeño o esté certificado por una autoridad acreditada conforme a su ordenamiento jurídico. 4. Las Partes fomentarán el uso interoperable de la firma electrónica avanzada o firma digital. 5. Las Partes arbitrarán los medios necesarios para la suscripción de acuerdos de reconocimiento mutuo de firma electrónica avanzada o digital."	-	Art. 14.6: "1. Salvo en circunstancias que se prevean de otra manera en su legislación, una Parte no podrá negar la validez legal de una firma únicamente sobre la base de que la firma está en forma electrónica. 2. Ninguna Parte adoptará o mantendrá medidas sobre autenticación electrónica que: (a) prohíban a las partes en una transacción electrónica el determinar mutuamente los métodos de autenticación adecuados para esa transacción; o (b) impidan a las partes en una transacción electrónica tener la oportunidad de probar ante las instancias judiciales o administrativas, que dicha transacción electrónica cumple con algún requerimiento legal de autenticación. 3. No obstante el párrafo 2, una Parte podrá requerir, para una categoría determinada de transacciones, que su método de autenticación cumpla con ciertos estándares de desempeño o que esté certificado por una autoridad acreditada conforme a su legislación. 4. Las Partes fomentarán la utilización de la interoperabilidad de la autenticación electrónica."

Protección al consumidor en línea	Art. 5: "Las Partes reconocen la importancia de proteger a los consumidores de prácticas comerciales fraudulentas y engañosas cuando participan en el comercio electrónico. En este sentido, cada Parte se ajustará, en materia de protección al consumidor en el comercio electrónico, a lo establecido en la normativa Mercosur vigente relacionada a la materia."	Art. 6.3: "Las Partes reconocen la importancia de medidas transparentes y efectivas para proteger a los consumidores de prácticas comerciales fraudulentas, que induzcan a error y engañosas cuando participan del comercio electrónico."	Art. 14.7: "1. Las Partes reconocen la importancia de adoptar y mantener medidas transparentes y efectivas para proteger a los consumidores de prácticas comerciales fraudulentas y engañosas tales como las señaladas en el Artículo 16.7.2 (Protección al Consumidor) cuando se involucran en el comercio electrónico. 2. Cada Parte adoptará o mantendrá leyes de protección al consumidor para prohibir actividades comerciales fraudulentas y engañosas que causen daño o un potencial daño a los consumidores que realicen actividades comerciales en línea. 3. Las Partes reconocen la importancia de la cooperación entre sus respectivas agencias de protección al consumidor u organismos nacionales relevantes en las actividades relacionadas con el comercio electrónico transfronterizo, a fin de mejorar el bienestar del consumidor. Con este fin, las Partes afirman que la cooperación que se busca bajo el Artículo 16.7.5 y el Artículo 16.7.6 (Protección al Consumidor) incluye la cooperación respecto de las actividades comerciales en línea."

Beneficios de proteger la información personal y su impacto en mejorar la confianza en el comercio digital	Art. 6.1: "Las Partes reconocen los beneficios de la protección de la información personal de los usuarios del comercio electrónico y la contribución que esto hace a la mejora de la confianza del consumidor en el comercio electrónico".	Art. 4.2.1: "Las Partes reconocen los beneficios económicos y sociales de la protección de la información personal de los participantes de la economía digital y la importancia de dicha protección en mejorar la confianza en la economía digital y el desarrollo del comercio."	Art. 14.8.1 "Las Partes reconocen los beneficios económicos y sociales de la protección de la información personal de los usuarios del comercio electrónico y la contribución que esto hace a la mejora de la confianza del consumidor en el comercio electrónico."
Marco legal de la protección de información personal, principios internacionales	Art. 6.2: "Las Partes deberán adoptar o mantener leyes, regulaciones o medidas administrativas para la protección de la información personal de los usuarios que participen en el comercio electrónico. A tales efectos tomarán en consideración los **estándares internacionales** que existen en esta materia, según lo previsto en el Artículo 2.5.(f)" Art. 2.5.(f): "garantizar la seguridad de los usuarios del comercio electrónico, así como su derecho a la protección de datos personales". Art. 2.5.(f) - Nota al pie 1: "Para mayor certeza, las Partes entienden que la recolección, el tratamiento y el almacenamiento de los datos personales se realizará siguiendo principios generales como previo consentimiento, finalidad, calidad, seguridad, responsabilidad, entre otros."	Art. 4.2.2: "Para tal fin, cada Parte adoptará o mantendrá un marco legal que disponga la protección de la información personal de los usuarios del comercio electrónico y digital. En el desarrollo de su marco legal para la protección de la información personal, cada Parte deberá tomar en consideración los **principios y directrices de los organismos internacionales pertinentes.**" Art. 4.2.2 - Nota al pie 1: "Para mayor certeza, una Parte podrá cumplir con la obligación de este párrafo adoptando o manteniendo medidas tales como **leyes que abarquen de manera amplia la privacidad**, información personal o protección de datos personales, **leyes sectoriales específicas** sobre protección de datos personales o privacidad, o **leyes que dispongan la aplicación de compromisos voluntarios de empresas** relacionados con la protección de datos personales o la privacidad." Art. 4.2.3. "Las partes reconocen que los principios que sostienen un marco legal robusto para la protección de la información personal deberían incluir:	Art. 14.8.2 "Para tal fin, cada Parte adoptará o mantendrá un marco legal para la protección de la información personal de los usuarios del comercio electrónico. En el desarrollo de su marco legal para la protección de la información personal, cada Parte deberá tener en consideración los principios y directrices de los organismos internacionales correspondientes. Art. 14.8.2 - Nota al pie 6: Para mayor certeza, una Parte podrá cumplir con la obligación en este párrafo adoptando o manteniendo medidas tales como la privacidad total, leyes sobre información personal o sobre protección de la información personal, leyes sectoriales sobre privacidad, o **leyes que prevean el ejercicio de compromisos voluntarios de las empresas** relacionadas con la privacidad."

		(a) limitación de recolección; (b) calidad de datos; (c) especificación de propósito; (d) limitación de uso; (e) salvaguardias de seguridad; (f) transparencia;(g) participación individual; y (h) rendición de cuentas."	
Aplicación no discriminatoria	Art. 6.3.: "Cada Parte deberá hacer los esfuerzos para asegurar que su marco legal doméstico para la protección de la información personal de los usuarios del comercio electrónico sea aplicado de una manera no discriminatoria."	Art. 4.2.4: "Cada Parte adoptará prácticas no discriminatorias al proteger a los usuarios del comercio electrónico de vulneraciones a la protección de la información personal ocurridas dentro de su jurisdicción."	Art. 14.8.3 "Cada Parte procurará adoptar prácticas no discriminatorias al proteger a los usuarios del comercio electrónico de violaciones a la protección de la información personal ocurridas dentro de su jurisdicción."
Publicación de información sobre la protección de la información personal	Art. 6.4: "Cada Parte publicará información sobre la protección de la información personal que proporciona a los usuarios del comercio electrónico, incluyendo como: (a) los individuos pueden ejercer sus derechos de acceso, rectificación y supresión; y (b) las empresas pueden cumplir con cualquier requisito legal."	Art. 4.2.5: "Cada Parte publicará información sobre la protección de la información personal que proporcione a los usuarios del comercio electrónico, incluyendo cómo: (a) los individuos pueden formular reclamaciones; y (b) las empresas pueden cumplir con cualquier requisito legal."	Art. 14.8.4 "Cada Parte deberá publicar la información relativa a la protección de la información personal que proporcione a los usuarios del comercio electrónico, incluyendo la manera en la que: (a) las personas pueden ejercer acciones; y (b) las empresas pueden cumplir con cualquier requisito legal."
Intercambio de información y experiencias en materia de protección de datos	Art. 6.5: "Las Partes deberán intercambiar información y experiencias en cuanto a su legislación de protección de la información personal."	Art. 4.2.7.: "Las Partes intercambiarán información sobre cómo los mecanismos mencionados en el párrafo 6 se aplican a sus respectivas jurisdicciones y explorarán formas para extender estos u otros arreglos adecuados para promocionar la compatibilidad y la interoperabilidad entre ellos."	Art. 14.8.5: "Reconociendo que las Partes pueden tener diferentes enfoques legales para proteger la información personal, cada Parte deberá fomentar el desarrollo de mecanismos que promuevan la compatibilidad entre sus diferentes regímenes. Estos mecanismos pueden incluir el reconocimiento de resultados regulatorios, ya sea de manera autónoma o por acuerdo mutuo, o de marcos internacionales más amplios. Con este fin, las Partes se esforzarán por intercambiar informa-

			ción sobre cualquiera de estos mecanismos aplicados en sus jurisdicciones y explorarán maneras de ampliar estos u otros medios adecuados para promover la compatibilidad entre estos."
Transferencia transfronteriza de información por medios electrónicos	Art. 7: "1. Las Partes reconocen que cada Parte podrá tener sus propios requisitos regulatorios sobre la transferencia de información por medios electrónicos, incluso con respecto a la protección de datos personales, según lo establecido en el Artículo 6. 2. Cada Parte permitirá la transferencia transfronteriza de información por medios electrónicos cuando esta actividad sea para la realización de la actividad comercial de una persona de una Parte. Para mayor certeza este párrafo estará sujeto al cumplimiento de lo dispuesto en el Artículo 6.7. 3. Nada de lo dispuesto en este Artículo impedirá que una Parte adopte o mantenga medidas incompatibles con el párrafo 2 para alcanzar un objetivo legítimo de política pública, siempre que la medida no se aplique de forma que constituya un medio de discriminación arbitraria o injustificable, o una restricción encubierta al comercio. 4. Este Artículo no se aplica a los servicios financieros."	Art. 4.3: "Las Partes afirman su nivel de compromisos en relación con la transferencia transfronteriza de información a través de medios electrónicos, en particular, pero no exclusivamente: ' 1. Las Partes reconocen que cada Parte podrá tener sus propios requisitos regulatorios sobre la transferencia de información por medios electrónicos. 2. Cada Parte permitirá la transferencia transfronteriza de información por medios electrónicos, incluyendo la información personal, cuando esta actividad sea para la realización de un negocio de una persona cubierta. 3. Nada de lo dispuesto en este Artículo impedirá que una Parte adopte o mantenga medidas incompatibles con el párrafo 2 para alcanzar un objetivo legítimo de política pública, siempre que la medida: (a) no se aplique de forma que constituya un medio de discriminación arbitraria o injustificable, o una restricción encubierta al comercio; y (b) no imponga restricciones a las transferencias de información mayores a las que se requieren para alcanzar el objetivo.'"	Art. 14.11 "Las Partes reconocen que cada Parte puede tener sus propios requisitos regulatorios relacionados con la transferencia de información por medios electrónicos. 2. Una Parte permitirá las transferencias transfronterizas de información por medios electrónicos, incluyendo la información personal, cuando esta actividad sea para la conducción de un negocio de una persona cubierta. 3. Nada en este Artículo impedirá que una Parte adopte o mantenga medidas incompatibles con el párrafo 2 para alcanzar un objetivo legítimo de política pública, siempre que la medida: (a) no se aplique de forma que constituya un medio de discriminación arbitrario o injustificable, o una restricción encubierta al comercio; y (b) no imponga restricciones a las transferencias de información mayores a las que se requieren para alcanzar el objetivo."

Ubicación de las instalaciones informáticas	Art. 8: "1. Las Partes reconocen que cada Parte podrá tener sus propios requisitos regulatorios relativos al uso de instalaciones informáticas, incluyendo los requisitos que buscan asegurar la seguridad y confidencialidad de las comunicaciones. 2. Una Parte no podrá exigir a una persona de otra Parte usar o ubicar las instalaciones informáticas en el territorio de esa Parte como condición para la realización de negocios en ese territorio. 3. Nada de lo dispuesto en este Artículo impedirá que una Parte adopte o mantenga medidas incompatibles con el párrafo 2 para alcanzar un objetivo legítimo de política pública, siempre que la medida no se aplique de forma que constituya un medio de discriminación arbitrario o injustificable, o una restricción encubierta al comercio. 4. Las Partes reconocen que usar o ubicar fuera de su territorio las instalaciones informáticas en las que alojen datos personales transferidos en virtud del Acuerdo constituye una transferencia internacional, en los términos del Artículo 7. 5. Este Artículo no se aplica a los servicios financieros."	Art. 4.4.: "Las Partes afirman su nivel de compromisos en relación con la ubicación de las instalaciones informáticas, en particular, pero no exclusivamente: " 1. Las Partes reconocen que cada Parte podrá tener sus propios requisitos regulatorios relativos al uso de instalaciones informáticas, incluyendo los requisitos que buscan asegurar la seguridad y confidencialidad de las comunicaciones. 2. Ninguna Parte podrá exigir a una persona cubierta usar o ubicar las instalaciones informáticas en el territorio de esa Parte, como condición para la realización de negocios en ese territorio. 3. Nada de lo dispuesto en este Artículo impedirá que una Parte adopte o mantenga medidas incompatibles con el párrafo 2 para alcanzar un objetivo legítimo de política pública, siempre que la medida: (a) no se aplique de forma que constituya un medio de discriminación arbitrario o injustificable, o una restricción encubierta al comercio; y (b) no imponga restricciones sobre el uso o ubicación de las instalaciones informáticas mayores a las que se requieren para alcanzar el objetivo."	Art. 14.13 1. "Las Partes reconocen que cada Parte puede tener sus propios requisitos reglamentarios relativos al uso de instalaciones informáticas, incluyendo los requisitos que buscan garantizar la seguridad y confidencialidad de las comunicaciones. 2. Ninguna Parte podrá exigir a una persona cubierta utilizar o ubicar las instalaciones informáticas en el territorio de esa Parte, como condición para la conducción de sus negocios en ese territorio. 3. Nada en este artículo impedirá que una Parte adopte o mantenga medidas incompatibles con el párrafo 1 para lograr un objetivo legítimo de política pública, siempre que la medida: (a) no se aplique de forma que constituya un medio de discriminación arbitrario o injustificable, o una restricción encubierta al comercio; y (b) no imponga restricciones sobre el uso o ubicación de las instalaciones informáticas mayores a las que se requieren para alcanzar el objetivo.

Principios sobre el acceso y el uso de Internet	Art. 9: "Las Partes reconocen los beneficios de que los consumidores en sus territorios tengan la capacidad de: (a) acceder y usar los servicios y aplicaciones de su elección disponibles en Internet 2; (b) conectar los dispositivos de usuario final de su elección a Internet, sujeto a los reglamentos técnicos de cada Parte; y (c) acceder a información sobre las prácticas de red del proveedor del servicio de acceso a Internet que puedan influir en la decisión del consumidor."	Art. 6.4: "Sujeto a las políticas, leyes y regulaciones aplicables, las Partes reconocen los beneficios de que sus consumidores tengan la capacidad de: (a) acceder y usar los servicios y aplicaciones a elección del consumidor disponibles en Internet, sujeto a una administración razonable de la red; (b) conectar a Internet los dispositivos de usuario final de elección del consumidor, siempre que dichos dispositivos no dañen la red; y (c) acceder a información sobre las prácticas de administración de redes del proveedor del servicio de acceso a Internet del consumidor."	Art. 14.10 "Sujeto a las políticas, leyes y reglamentaciones aplicables, las Partes reconocen los beneficios de que los consumidores en sus territorios tengan la posibilidad de: (a) acceder y utilizar los servicios y aplicaciones de su elección disponibles en Internet, sujeto a una administración razonable de la red 7; (b) conectar los dispositivos de usuario final de su elección a Internet, siempre y cuando dichos dispositivos no dañen la red; y (c) acceder información sobre prácticas de administración de redes de los proveedores de servicios de acceso a Internet de los consumidores."
Cooperación	Art. 12. "Reconociendo la naturaleza global del comercio electrónico, las Partes afirman la importancia de: (a) trabajar conjuntamente para facilitar el uso del comercio electrónico, generar mejores prácticas para aumentar las capacidades de realizar negocios, colaborar y cooperar en cuestiones técnicas y de asistencia para maximizar las oportunidades de las micro, pequeñas y medianas empresas; (b) compartir información y experiencias sobre leyes, regulaciones, políticas, y programas en la esfera del comercio electrónico, incluyendo aquéllos relacionados con la protección de la información personal; protección del consumidor, seguridad en las comunicaciones electrónicas, reconocimiento y facilitación de la inteporalidad de firmas electrónicas	(texto no equivalente)	Art. 14.15: "Reconociendo la naturaleza global del comercio electrónico, las Partes se esforzarán en: (a) trabajar conjuntamente para apoyar a las micro, pequeñas y medianas empresas a superar los obstáculos que se encuentren en su utilización; (b) compartir información y experiencias sobre regulaciones, políticas, aplicación y cumplimiento relativo al comercio electrónico, incluyendo: (i) protección de la información personal; (ii) protección de los consumidores en línea que incluyan medios de retribución a los consumidores y mejoren la confianza del consumidor; (iii) mensajes electrónicos comerciales no solicitados; (iv) seguridad en las comunicaciones electrónicas; (v) autenticación; y (vi) e-gobierno; (c) intercambiar información

	transfronterizas, incluso firmas electrónicas avanzadas o firmas digitales, autenticación electrónica, localización de servidores, derechos de propiedad intelectual, gobierno electrónico, e iniciativas para el fomento y difusión del acceso y uso del comercio electrónico por parte de las micro, pequeñas y medianas empresas; (c) intercambiar información y compartir puntos de vista sobre el acceso del consumidor a productos y servicios que se ofrecen en línea entre las Partes; (d) participar activamente en foros regionales y multilaterales para promover el desarrollo del comercio electrónico; (e) **fomentar el desarrollo por parte del sector privado de los métodos de autorregulación que fomenten el comercio electrónico, incluyendo códigos de conducta, contratos modelo, directrices y mecanismos de cumplimiento**; [...]		y compartir puntos de vista sobre el acceso del consumidor a productos y servicios que se ofrecen en línea entre las Partes; (d) participar activamente en foros regionales y multilaterales para promover el desarrollo del comercio electrónico; y (e) promover el desarrollo por parte del sector privado de los métodos de autorregulación que fomenten el comercio electrónico, incluyendo códigos de conducta, contratos modelo, directrices y mecanismos de aplicación."

8. Notas

1 / Destacamos que, a la fecha de finalización de este trabajo (junio de 2022), el Acuerdo aún no entró en vigor. Según el Artículo 14 del Acuerdo, el documento entrará en vigor treinta (30) días después del depósito del instrumento de ratificación por el segundo Estado Parte del Mercosur. A la fecha, únicamente Uruguay ha depositado su respectivo instrumento. https://www.mercosur.int/documento/acuerdo-sobre-comercio-electronico-del-mercosur/

2 / Acuerdo, Art. 5.

3 / Acuerdo, Art.8.

4 / Acuerdo, Art. 2.

5 / A los fines del presente trabajo utilizaremos los términos comercio electrónico y comercio digital de forma indistinta, y tomando como definición la de la Organización Mundial del Comercio que lo define como: "la producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos". Para más información sobre la definición, puede consultase el siguiente enlace: https://www.wto.org/spanish/tratop_s/ecom_s/ecom_s.htm

6 / Mateo Ceurvels, "Latin America Ecommerce Forecast 2021", Insider Intelligence, eMarketers, Julio 2021, disponible en https://www.emarketer.com/content/latin-america-ecommerce-forecast-2021 (la traducción nos pertenece), pág 1.

7 / S. Herreros, "La regulación del comercio electrónico transfronterizo en los acuerdos comerciales: algunas implicaciones de política para América Latina y el Caribe", serie Comercio Internacional, N° 142 (LC/TS.2019/42), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2019, pag 5.

8 / En este trabajo, incluimos a las microempresas dentro del término "PYMEs".

9 / Sin perjuicio de que la cuantificación del comercio electrónico plantea grandes desafíos metodológicos, y que las estadísticas disponibles no suelen ser comparables entre sí, las estimaciones disponibles sugieren que en los países del Mercosur, puede afirmarse que dicho comercio viene aumentando año tras año. Para más información sobre la evolución del comercio electrónico en los países del Mercosur, tanto desde la perspectiva de la oferta como de la demanda, nos remitimos para Argentina a los informes anuales de la Cámara Argentina de Comercio Electrónico, disponibles en https://www.cace.org.ar/estadisticas, para Brasil, https://www.ebit.com.br/webshoppers, para Paraguay https://www.capace.org.

py/blog/categories/estadisticas, y para Uruguay de la Cámara de Economía Digital del Uruguay, disponibles en https://www.cedu.org.uy/informes.

10 / Mateo Ceurvels, "Latin America Ecommerce Forecast 2021", Insider Intelligence, eMarketers, Julio 2021 disponible en https://www.emarketer.com/content/latin-america-ecommerce-forecast-2021.

11 / Ibidem

12 / En este mismo sentido, S. Herreros indica que "Sin perjuicio de las especificidades nacionales, América Latina y el Caribe muestra considerables rezagos en su inserción en la economía digital", en "La regulación del comercio electrónico transfronterizo en los acuerdos comerciales: algunas implicaciones de política para América Latina y el Caribe", serie Comercio Internacional, N° 142, (LC/TS.2019/42), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2019, Pág 7.

13 / "La regulación del comercio electrónico transfronterizo en los acuerdos comerciales: algunas implicaciones de política para América Latina y el Caribe", serie Comercio Internacional, N° 142, (LC/TS.2019/42), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2019, Pág 13.

14 / Para más información sobre el impacto del COVID-19 en el Comercio Electónico a nivel global nos remitimos al informe de la Comisión de Naciones Unidas para Derecho Mercantil Internacional (CNUDMI en español o UNCTAD, en inglés) disponible aquí https://unctad.org/system/files/official-document/tn_unctad_ict4d18_en.pdf.

15 / Mateo Ceurvels, "Latin America Ecommerce Forecast 2021", Insider Intelligence, eMarketers, Julio 2021 disponible en https://www.emarketer.com/content/latin-america-ecommerce-forecast-2021 (la traducción nos pertenece). Pág. 1.

16 / Ibidem, pág 2.

17 / Ibidem, pág 9.

18 / Kantar Insights "Los Argentinos y el eCommerce: cómo vendemos y compramos online" preparado por la Cámara Argentina de Comercio Electrónico. Pág 16.

19 / Mateo Ceurvels, "Latin America Ecommerce Forecast 2021", Insider Intelligence, eMarketers, Julio 2021 disponible en https://www.emarketer.com/content/latin-america-ecommerce-forecast-2021, pág 21.

20 / Kantar Insights "Los Argentinos y el eCommerce: cómo vendemos y compramos online" preparado para la Cámara Argentina de Comercio Electrónico, pags. 150 y 151.

21 / S. Herreros, "La regulación del comercio electrónico transfronterizo en los acuerdos comerciales: algunas implicaciones de política para América Latina y el Caribe", serie Comercio

Internacional, N° 142(LC/TS.2019/42), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2019, pág. 11.

22 / S. Herreros, "La regulación del comercio electrónico transfronterizo en los acuerdos comerciales: algunas implicaciones de política para América Latina y el Caribe", serie Comercio Internacional, N° 142 (LC/TS.2019/42), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2019, pag. 13.

23 / Argentina bajo la Resolución de la Secretaría de Comercio Interior del Ministerio de Desarrollo Productivo N° 270/2020 del MDP del 04/09/20, publicada en el BO el 08/09/20; Brasil a través del Decreto N° 10.271 del 06/03/20, publicado en el DOU el 09/03/20; Paraguay a través del Decreto de la Presidencia de la República N° 4053 del 15/09/20; y Uruguay a través del Decreto del PE Nº 167/021 del 02/06/21, publicado en el DO el 08/06/21. Información disponible en: **https://normas.mercosur.int/public/normativas/3768**.

24 / Ratificado por Argentina y Uruguay. Entró en vigencia el 13 de agosto del 2021, **https://www.mercosur.int/acuerdo-de-reconocimiento-mutuo-de-firmas-digitales-en-el-mercosur/** y **https://www.mre.gov.py/tratados/public_web/ConsultaMercosur.aspx**

25 / Las iniciativas correspondientes a la Agenda de este Grupo se encuentran disponibles en el siguiente link: **https://www.mercosur.int/temas/agenda-digital/**.

26 / Ratificado por Argentina. Entra en vigencia en agosto del 2021 **https://www.mre.gov.py/tratados/public_web/DetallesTratado.aspx?id=o1dBpUe2l7MGQuG0qA/Cmw==** , **https://www.mercosur.int/acuerdo-de-reconocimiento-mutuo-de-firmas-digitales-en-el-mercosur/**

27 / Resolución MERCOSUR 37/19 disponible en: **https://normas.mercosur.int/public/normativas/3768**

28 / Argentina bajo la Resolución de la Secretaría de Comercio Interior del Ministerio de Desarrollo Productivo N° 270/2020 del MDP del 04/09/20, publicada en el BO el 08/09/20; Brasil a través del Decreto N° 10.271 del 06/03/20, publicado en el DOU el 09/03/20; Paraguay a través del Decreto de la Presidencia de la República N° 4053 del 15/09/20; y Uruguay a través del Decreto del PE Nº 167/021 del 02/06/21, publicado en el DO el 08/06/21. Información disponible en: **https://normas.mercosur.int/public/normativas/3768**.

29 / El texto no ha sido ratificado y no se encuentra vigente, estando disponible en el siguiente link **https://www.cancilleria.gob.ar/es/acuerdo-mercosur-ue. La subsección 6 refiere al comercio electrónico**.

30 / Posible Acuerdo Mercosur Unión Europea, Art.42.

31 / Posible Acuerdo Mercosur Unión Europea, Art. 46.

32 / Posible Acuerdo Mercosur Unión Europea, Art. 47.

33 / Posible Acuerdo Mercosur Unión Europea, Art. 48.

34 / Posible Acuerdo Mercosur Unión Europea, Art. 48.

35 / Véase "Chile-Uruguay, Acuerdo de Libre Comercio", en **https://www.subrei.gob.cl/acuerdos-comerciales/acuerdos-comerciales-vigentes/uruguay**

36 / Véase "Chile-Argentina, Acuerdo Comercial", en "**https://www.subrei.gob.cl/acuerdos-comerciales/acuerdos-comerciales-vigentes/argentina**.

37 / Acuerdo , Art.1.

38 / Acuerdo de Libre Comercio entre Argentina y Chile, disponible en **https://www.subrei.gob.cl/docs/default-source/acuerdos/argentina/texto-acuerdo-de-libre-comercio-chile-argentina.pdf?sfvrsn=da8b6d7_2**, y Acuerdo de Libre Comercio entre Uruguay y Chile, disponible en **https://www.subrei.gob.cl/docs/default-source/acuerdos/uruguay/texto-alc-chile-uruguay.pdf?sfvrsn=85b8e4a5_0**.

39 / Acuerdo sobre Comercio Electrónico del Mercosur. Art. 2.5.b, d y f respectivamente.

40 / Argentina bajo la Resolución de la Secretaría de Comercio Interior del Ministerio de Desarrollo Productivo N° 270/2020 del MDP del 04/09/20, publicada en el BO el 08/09/20; Brasil a través del Decreto N° 10.271 del 06/03/20, publicado en el DOU el 09/03/20; Paraguay a través del Decreto de la Presidencia de la República N° 4053 del 15/09/20; y Uruguay a través del Decreto del PE Nº 167/021 del 02/06/21, publicado en el DO el 08/06/21. Información disponible en: **https://normas.mercosur.int/public/normativas/3768**.

41 / Las medidas de seguridad y los mecanismos de anonimización o disociación representan un desafío tanto para los responsables del cumplimiento como para los reguladores que deben reglamentarlas y/o auditarlas, atendiendo al constante desarrollo tecnológico. Así, por ejemplo, las medidas de seguridad pueden devenir vulnerables con el paso del tiempo o un mecanismo de anonimización puede ser suficiente en determinado momento y volverse obsoleto al tiempo.

42 / Acuerdo Art 2.5.(b): "Considerando el potencial del comercio electrónico como un instrumento de desarrollo social y económico, las Partes reconocen la importancia de: [...] (b) alentar la autorregulación en el sector privado para promover la confianza y la seguridad jurídica en el comercio electrónico, teniendo en cuenta los intereses y los derechos de los usuarios, a través de iniciativas tales como las directrices, modelos de contratos, códigos de conducta y sellos de confianza."

43 / En principio, bajo la normativa local argentina existe una prohibición de transferir datos personales a países que no proporcionen niveles de protección adecuados (el Art. 12 de la Ley de Protección de Datos Personales Nº 25.326 dicta que "Es prohibida la transferencia de

datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.”). No obstante, el Decreto Decreto Reglamentario 1558/2001 aclara que “(...)Se entiende que un Estado u organismo internacional proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación, o del amparo que establezcan las cláusulas contractuales que prevean la protección de datos personales.”. En este marco, la entonces Dirección Nacional de Protección de Datos Personales (hoy incluida bajo la estructura de la Agencia de Acceso a la Información Pública) emitió la Disposición 60E/2016 que dispone cláusulas modelos para los contratos de transferencia internacional de datos a países no adecuados y la Agencia de Acceso a la Información Pública estableció mediante la Resolución 159/2018 los lineamientos y contenidos básicos de las normas corporativas vinculantes que regulen dichas transferencias. Cabe mencionar que en caso de que los documentos en cuestión no cumplan con los requisitos dispuestos en estas normas, se deberá requerir la aprobación de la Agencia de Acceso a la Información Pública previo a la transferencia de datos personales a jurisdicciones que no garanticen niveles de protección adecuados.

44 / Como posibles ejemplos de lo aquí dispuesto puede citarse proyectos de ley de soberanía de datos personales como el presentado en Argentina por los diputados y diputadas Sandra Mendoza, Adrián Grana, Carlos Castagneto, Eduardo Seminara, Juan Manuel Huss y Rodrigo Martín Rodríguez (Expediente 0526-D-2017) que pretendía regular los datos producidos por el Estado Nacional estableciendo que deben ser almacenados en el territorio argentino. Proyecto disponible en: **https://www.hcdn.gob.ar/proyectos/textoCompleto.jsp?exp=0526-D-2017&tipo=LEY**

45 / Acuerdo. Art. 7.4

46 / CPTPP Capítulo 11 que regula la materia específicamente, y Art. 1.12 del DEPA que excluye a los servicios financieros.

47 / Ley de Protección de Datos Personales Nº25.326, Art. 12 inc. c. y Ley de Protección de Datos Personales 18.331 Art.23 inc.3.

48 / PROYECTO-D-2162170 de Ley Protección de Datos Personales en Paraguay. Art. 57. **http://silpy.congreso.gov.py/expediente/123459**

49 / Acuerdo. Art. 8.1.

50 / Acuerdo. Art. 8.2.

51 / Acuerdo. Art. 8.3.

52 / Acuerdo. Art. 8.3.

53 / Sebastián Herrero identifica este tipo de requisitos de almacenar ciertos datos en

servidores locales y/o de desarrollar infraestructura local para ese fin como una barrera al desarrollo del comercio electrónico en la región. S. Herreros: "La regulación del comercio electrónico transfronterizo en los acuerdos comerciales: algunas implicaciones de política para América Latina y el Caribe", serie Comercio Internacional, N° 142 (LC/TS.2019/42), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2019. Disponible en **https://repositorio.cepal.org/bitstream/handle/11362/44667/1/S1900451_es.pdf**

54 / Proyecto de Ley 0526-D-2017 presentados por los diputados y diputadas Sandra Mendoza, Adrián Grana, Carlos Castagneto, Eduardo Seminara, Juan Manuel Huss y Rodrigo Martín Rodríguez. Disponible en **https://www.hcdn.gob.ar/proyectos/resultados-buscador.html**

55 / Acuerdo. Art. 10.1

56 / Art. 48: "Unsolicited direct marketing communications 1. Each Party shall endeavour to protect end-users effectively against unsolicited direct marketing communications. To this end, in particular the following paragraphs shall apply. 2. Each Party shall endeavour to ensure that natural and juridical persons do not send direct marketing communications to consumers who have not given their consent 23. 3. Notwithstanding paragraph 2, the Parties shall allow natural and juridical persons which have collected, in accordance with each Party's own laws and regulations, a consumer's contact details in the context of the sale of a product or a service, to send direct marketing communications to that consumer for their own similar products or services. 4. Each Party shall endeavour to ensure that direct marketing communications are clearly identifiable as such, clearly disclose on whose behalf they are made, and contain the necessary information to enable end-users to request cessation free of charge and at any moment." Disponible en **https://trade.ec.europa.eu/doclib/docs/2019/july/tradoc_158159.%20Services%20and%20Establishment.pdf**.

57 / Acuerdo. Art. 10.2

58 / Información del evento mencionado en su edición de 2019 se encuentra disponible en **http://emailsummit.org/2019/** mientras que la información de todas las ediciones del evento se encuentra disponible en **http://emailsummit.org/**

59 / Entendemos que la regulación llega tarde sobre todo en la práctica de garantizar el consentimiento de los usuarios para recibir comunicaciones comerciales directas no solicitadas y en cuanto al cumplimiento con el estándar de mínima del derecho de retiro o bloqueo como práctica generalizada, bien implementada. Sumado a esto, advertimos que en la región pareciera no contar con mecanismos de enforcement adecuados para casos de incumplimiento.

60 / A modo de ejemplo, nos parece relevante citar el siguiente artículo, Michael Veale and

Frederik Zuiderveen Borgesius, 'Adtech and Real-Time Bidding under European Data Protection Law', 2021, German Law Journal. disponible en https://osf.io/preprints/socarxiv/wg8fq/ que analiza la complejaa relación entre los sistemas de tecnología publicitaria contemporánea, que sustenta gran parte de sus desarrollos en el perfilamiento de los usuarios basado en su comportamiento en línea y a través de aplicaciones móviles, con relación a la base legal para el tratamiento, la transparencia y la seguridad exigidos por la normativa europea de protección de datos personales vigente (GDPR).

61 / Para más información sobre esta iniciativa disponible en https://mydata.org/

62 / De Mooy, M. (2017). Rethinking privacy self-management and data sovereignty in the age of big data: Considerations for future policy regimes in the United States and the European Union. Bertelsmann Stiftung.

63 / Acuerdo. Art. 12.a.

64 / Decisión CMC N° 37/03, que aprueba el Reglamento del Protocolo de Olivos para la Solución de Controversias en el Mercosur. El Protocolo de Olivos puede encontrarse en https://www.tprmercosur.org/es/docum/Protocolo_de_Olivos_es.pdf.

65 / Información oficial disponible en https://www.mercosur.int/quienes-somos/solucion-controversias/

66 / De Mooy, M. (2017). Rethinking privacy self-management and data sovereignty in the age of big data: Considerations for future policy regimes in the United States and the European Union. Bertelsmann Stiftung.

67 / Ibidem.

68 / Hirsch, D. D. (2010). The law and policy of online privacy: Regulation, self-regulation, or co-regulation. Seattle UL Rev., 34, 439.

69 / Ibidem.

70 / Ibidem.

71 / Listokin, S. (2015). Industry Self-Regulation of Consumer Data Privacy and Security, 32 J. Marshall J. Info. Tech. & Privacy L. 15 (2015). The John Marshall Journal of Information Technology & Privacy Law, 32(1), 2.

72 / OECD. Industry Self-Regulation: Role and Use in Supporting Consumer Interests. Organization for Economic Cooperation and Development, March 2015. citado en e Mooy, M. (2017). Rethinking privacy self-management and data sovereignty in the age of big data: Considerations for future policy regimes in the United States and the European Union. Bertelsmann Stiftung.

73 / Hirsch, D. D. (2010). The law and policy of online privacy: Regulation, self-regulation, or co-

regulation. Seattle UL Rev., 34, 439.

74 / Hirsch, D. D. (2010). The law and policy of online privacy: Regulation, self-regulation, or co-regulation. Seattle UL Rev., 34, 439..

75 / De Mooy, M. (2017). Rethinking privacy self-management and data sovereignty in the age of big data: Considerations for future policy regimes in the United States and the European Union. Bertelsmann Stiftung.

76 / Co-regulación es un término acuñado por cierta parte de la doctrina que refiere iniciativas regulatorias en las que participan el gobierno y la industria, compartiendo responsabilidad de redactar y aplicar normas reguladoras. Así, Dennis D. Hirsch lo describe como un sistema regulatorio híbrido. Hirsch, D. D. (2010). The law and policy of online privacy: Regulation, self-regulation, or co-regulation. Seattle UL Rev., 34, 439.

77 / En relación con la cuestión de la reclamación en línea, durante 2015 el Sello Hot Sale (CACE) del programa eConfianza ofreció la integración con una plataforma de Online Dispute Resolution - Resolución de Disputas en Línea- denominada Pactanda, como prueba piloto, para canalizar los reclamos de los consumidores durante el evento de ventas masivas online denominado Hot Sale de Argentina, coordinado por la Cámara Argentina de Comercio Electrónico (CACE). Los resultados de esta experiencia piloto fueron presentados en el evento eCommerce Day 2015 organizado por el eCommerce Instituto y la Cámara Argentina de Comercio Electrónico en la sección "Buenas Prácticas y Generación de Confianza en el Canal Online, Caso de Éxito de Posventa con Sello Hot Sale y Pactanda: Casa del Audio", disponible en **https://www.ecommerceday.org.ar/2015/presentaciones-2015/**.

78 / Para más información acerca de la historia de los Sellos de Confianza de la Asociación de Internet de MX, visitar el siguiente **https://sellosdeconfianza.org.mx/?op=que**

79 / Para más información sobre los Sellos Regionales eConfianza en **https://ecommerce.institute/econfianza/** y **https://fr.slideshare.net/einstituto/presentacin-sellos-econfianza-2013**

80 / Las acciones de difusión de los Sellos CACE incluyeron eventos de capacitación para las Empresas del sector, como puede observarse, por ejemplo, en el evento realizado en abril del 2012 organizado por la Cámara Argentina de Comercio Electrónico en la Universidad de Palermo, de la Ciudad de Buenos Aires, Argentina: **https://www.cace.org.ar/agenda-e-commerce-seminario-abril** en el que se habló de generación de confianza y de resolución electrónica de disputas. Y en el evento de noviembre de 2013 de presentación de los mismos Sellos **http://www.einstituto.org/site/2811-invitacion-desayuno-sellos-cace/** en el que se presentó el tema de los Códigos de buenas prácticas y la autorregulación en Internet.

81 / Disposición 4/2004 que homologa el Código de Ética de la Asociación de Marketing Directo e Interactivo de Argentina, disponible en **http://servicios.infoleg.gob.ar/infolegInternet/anexos/100000-104999/101360/norma.htm**

82 / **https://distintivodigital.profeco.gob.mx/**

83 / **https://distintivodigital.profeco.gob.mx/info-codigo-de-etica.php**

84 / La lista completa de los requisitos que se solicitan a las empresas para poder adherirse están enumerados en este enlace **https://distintivodigital.profeco.gob.mx/info-codigo-de-etica.php**

85 / Por ejemplo, en el Proyecto de Ley presentado por el Senador Dalmacio E. Mera disponible en el siguiente link: **https://www.senado.gob.ar/parlamentario/comisiones/verExp/2986.20/S/PL**. Este proyecto de ley recepta aquel enviado al Congreso en el 2018 por el Poder Ejecutivo que había sido elaborado por la Agencia de Acceso a la Información Pública y sometido a la consulta de partes interesadas (ese se puede consultar en el siguiente link **https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales**).

86 / LPDPA . Art. 4. inc. 1

87 / LPDPA . Art. 4. inc. 3

88 / LPDP. Art. 11 inc. 4

89 / Decisión de la Comisión C (2003) 1731 de fecha 30 de junio de 2003 con arreglo a la Directiva 95/46/CE

90 / Algunos ejemplos de esta normativa son la Resolución N° 40/2018 referente a la Política Modelo de Protección de Datos Personales para Organismos Públicos y al Delegado de Protección de Datos Personales; la Resolución N°47/2018 sobre Medidas de Seguridad; la Resolución N° 159/2018, mediante la cual se aprobó unos lineamientos y contenidos básicos que las empresas pueden incorporar a sus normas autorregulatorias (a modo de binding corporate rules), entre otras. Además, Argentina ratificó el Convenio de Protección para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, Estrasburgo, 28.I.1981, conocido como "Convenio 108" el que se tratará en un apartado específico de este documento.

91 / LPDPA . Art. 9 inc. 1

92 / LPDPA . Art. 9 inc. 2

93 / LPDP. Art. 12 inc. 1: "Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados."

94 / La Dirección Nacional de Protección de Datos Personales (actualmente incluida bajo la estructura de la Agencia de Acceso a la Información Pública) mediante la Disposición 60e/2016 establece que los países que cumplen con niveles adecuados de protección conforme la legislación argentina son: los Estados miembros de la Unión Europea y miembros del espacio económico europeo (EEE), Confederación Suiza, Guernsey, Jersey, Isla de Man, Islas Feroe, Canadá sólo respecto de su sector privado, Principado de Andorra, Nueva Zelanda, República Orietal del Uruguay y Estado de Israel sólo respecto de los datos que reciban un tratamiento automatizado. Esta disposición fue modificada por la Agencia de Acceso a la Información Pública en 2019 a fin de incorporar expresamente al Reino Unido de Gran Bretaña e Irlanda del Norte.

95 / LPDPA, Art. 12. Inc. 2. d.

96 / LPDPA, Art. 12 Inc. 2. e.

97 / Resolución de la Agencia de Acceso a la Información Pública N° 159/2018 disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/317228/norma.htm

98 / Disposición 60E/2016 emitida por la Dirección Nacional de Protección de Datos Personales, autoridad de control antecesora de la Agencia de Acceso a la Información Pública http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm

99 / Decreto Reglamentario de la Ley 25326 N°1558/2001, que se encuentra disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/norma.htm

100 / Disposición 4/2009 de la Dirección Nacional de Protección de Datos Personales, autoridad de aplicación antecesora de la AAIP, disponible en https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-4-2009-151221/texto

101 / LGPDP. Art. 6, I.

102 / LGPDP. Art. 6, II.

103 / LGPDP. Art. 6, III.

104 / LGPDP. Art. 6, V.

105 / LGPDP. Art. 6, X.

106 / LGPDP. Art. 42, 1, I.

107 / LGPDP. Art. 7, I

108 / LGPDP. Art. 8, 4.

109 / LGPDP. Art. 8, 2.

110 / LGPDP. Art. 6, VII.

111 / LGPDP. Art. 40, 46 y 49.

112 / LGPDP. Art. 44.

113 / LGPDP. Art. 33.

114 / LGPDP. Art. 35.

115 / LGPDP. Art. 7.

116 / Information Commissioner's Office. Privacy and Electronic Communications Regulations. Direct Marketing. https://ico.org.uk/media/1555/direct-marketing-guidance.pdf

117 / Ley Nº 6534 disponible en https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-de-datos-personales-crediticios

118 / Ley Nº 6534. Art. 3.

119 / Al respecto cabe mencionar que se han presentado proyectos de Ley que buscarían alinear la regulación en materia de protección de datos personales al estándar europeo. http://www.diputados.gov.py/index.php/noticias/presentan-proyecto-de-ley-que-garantizara-la-proteccion-de-los-datos-personales-en-nuestro-pais

120 / Ley Nº 6534, Art. 10.

121 / Ley Nº 4868. Texto disponible en https://www.bacn.gov.py/leyes-paraguayas/961/ley-n-4868-comercio-electronico

122 / Ley Nº 4868, Art. 23.

123 / Ley 18.331. Disponible en: https://www.impo.com.uy/bases/leyes/18331-2008

124 / Decreto Reglamentario 414/009. Disponible en https://www.impo.com.uy/bases/leyes/18331-2008

125 / La Ley 19.670 incorpora disposiciones específicas en materia de protección de datos personales en sus artículos 37 a 40. Texto Disponible en: https://legislativo.parlamento.gub.uy/htmlstat/pl/leyes/Ley19670.pdf. En relación a esta norma cabe mencionar que su Decreto Reglamentario Nº 64/020 refiere expresamente a que el mismo se dicta tomando en consideración "Reglamento Europeo N° 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, los Estándares en Protección de Datos Personales para los Estados Iberoamericanos emitidos por la Red Iberoamericana de Protección de Datos en junio de 2017, el Convenio N° 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, su Protocolo Adicional de 8 de noviembre de 2001 -ambos aprobados por Ley N° 19.030 de 27 de diciembre de 2012-, y el Protocolo de Modernización del citado Convenio aprobado por el Comité de Ministros del Consejo de Europa el 18 de mayo de 2018, suscrito por la República Oriental del Uruguay el 10 de octubre de 2018", Texto disponible

en: https://www.impo.com.uy/bases/decretos/64-2020

126 / Resolución 32/2020 de la Unidad Reguladora y de Control de Datos Personales. Disponible en: https://www.gub.uy/unidad-reguladora-control-datos-personales/sites/unidad-reguladora-control-datos-personales/files/2020-05/Resoluci%C3%B3n%2032-%202020.pdf

127 / Información Oficial disponible en: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/uruguay-ratifico-convencion-108-modernizada

128 / LPDPU, Capítulo II.

129 / LPDPU, Art. 5.

130 / LPDPU, Art. 6.

131 / LPDPU, Art. 7

132 / LPDPU, Art. 8.

133 / LPDPU. Art. 11.

134 / Argentina lo ratificó mediante Ley 27.483

135 / Países que lo han ratificado disponible en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?module=treaty-detail&treatynum=223

136 / Estados Partes del Convenio 108 disponible en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?module=signatures-by-treaty&treatynum=108

137 / En el cuadro comparativo disponible en el sitio oficial se destacan las diferencias entre uno y otro texto: https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958

138 / Convenio 108. Art. 4.

139 / Convenio 108. Art. 5.

140 / Convenio 108. Art. 7.

141 / Convenio 108. Art. 7.1.

142 / Ley 19.670, Art. 38.

143 / Convenio 108+ Art. 14.

144 / Red Iberoamericana de Protección de Datos Personales. Estándares de Protección de Datos Personales. Disponible en https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

145 / Respecto de Uruguay la Ley 19.670 que introduce modificaciones a la LPDPU refiere

expresamente a que ha considerado estos estándares y lo mismo sucede con los proyectos de reforma de ley en Argentina citados en este documento.

146 / Acuerdo 6.2."Las Partes deberán adoptar o mantener leyes, regulaciones o medidas administrativas para la protección de la información personal de los usuarios que participen en el comercio electrónico. A tales efectos tomarán en consideración los estándares internacionales que existen en esta materia, según lo previsto en el Artículo 2.5.(f)"

147 / Capítulo II. Punto 11.

148 / Punto 15.

149 / Punto 16.

150 / Punto 20.

151 / Punto 20.3.

152 / Punto 21.1.

153 / Punto 21.2.

154 / Punto 22.1 y 22.2.

155 / Punto 22.4.

156 / Punto 23.

157 / Punto 24.

158 / Punto 24 y 30.

159 / Punto 29.

160 / Punto 31.

161 / Punto 24.2.

162 / Punto 25.

163 / Punto 26.

164 / Punto 27.

165 / Punto 28.

166 / Este tipo de mecanismo resulta esencial para la inclusión financiera en países en los que existen amplios segmentos de la población de la región que se encuentran excluidas de la posibilidad de obtener créditos del sistema bancario tradicional (por no calificar crediticiamente para estos créditos).

167 / Para conocer algunos ejemplos de este tipo de tratamiento realizado por los bancos digitales y las fintech no remitimos a la siguiente nota **https://www.iproup.com/finanzas/7020-fintech-cuenta-machine-learning-Por-que-bancos-digitales-usan-redes-sociales-para-dar-creditos**

168 / Punto 29.2.

169 / Punto 29.3.

170 / Punto 29.4.

171 / Punto 30.

172 / Punto 30.2.

173 / Punto 30.4

174 / Punto 31.

175 / Punto 32.2.

176 / Punto 32.3.

177 / Cabe mencionar que si está previsto bajo la regulación en Argentina (Ley 25.326 Art. 14.4) y Uruguay (Ley 18.331 Art. 14).

178 / Punto 36.1.

179 / Punto 36.2.

180 / Capítulo VI

181 / Punto 38.1.

182 / Guía Para la Elaboración de Evaluaciones de Impacto. Disponible en: **https://www.argentina.gob.ar/noticias/argentina-y-uruguay-lanzan-la-guia-evaluacion-de-impacto-en-la-proteccion-de-datos**

183 / Punto 39.

184 / Tener en cuenta que estos mecanismos de autorregulación son complementarios a la regulación vigente por lo que se entrañan en un sistema de co-regulación.

185 / Punto 40.

186 / Punto 40.2

187 / Punto 40.3

188 / Por ejemplo, en el documento que elaboraron las autoridades de Argentina y Uruguay se establece una guía para la elaboración de evaluaciones de impacto, sin embargo, esto no resulta a la fecha de este informe obligatorio para los responsables del tratamiento. **https://www.argentina.gob.ar/noticias/argentina-y-uruguay-lanzan-la-guia-evaluacion-de-impacto-en-la-proteccion-de-datos**

189 / Punto 41.

190 / Ley General de Protección de Datos Personales No. 13.709, Art. 38.

191 / En idioma español se lo denomina "Acuerdo de Asociación de Economía Digital", y su texto está disponible en el siguiente enlace: **https://www.subrei.gob.cl/docs/default-source/acuerdos/depa/depa-es.pdf?sfvrsn=4122158b_2**

192 / Gobierno de Canadá, "Background: Canada's possible accession to the Digital Economy

Partnership Agreement" en https://www.international.gc.ca/trade-commerce/consultations/depa-apen/background-information.aspx?lang=eng

193 / Véase el portal del Ministry of Trade and Industry Singapore en https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement.

194 / El Acuerdo, por ejemplo, menciona a las pequeñas y medianas empresas en el Art. 2.5.(e) pero no prevé un capítulo detallado al respecto como lo hace el DEPA en el Módulo 10, donde establece hasta un "Diálogo Digital" para Pymes.

195 / Acuerdo, Art. 1; DEPA, Art.1.3.

196 / DEPA Art. 4.2.1, Acuerdo Art. 6.1.

197 / DEPA Art. 4.2.2 y su nota al pie, 4.2.3, Acuerdo Art. 6.2, Art. 2.5.(f) y su nota al pie.

198 / DEPA Art. 4.2.4, Acuerdo Art. 6.3.

199 / DEPA Art. 4.2.5, Acuerdo Art. 6.4.

200 / DEPA Art. 4.2.7, Acuerdo Art. 6.5.

201 / DEPA Art. 4.3, Acuerdo Art. 7.

202 / DEPA Art. 4.4, Acuerdo Art. 8.

203 / DEPA Art. 6.3.1, Acuerdo Art. 5.

204 / Por ejemplo, a la Resolución 037-2019 del Mercosur sobre Protección del Consumidor Comercio Electrónico, disponible en https://normas.mercosur.int/simfiles/normativas/73867_RES_037-2019_ES_Protecci%C3%B3n%20Consumidor%20Comercio%20Electr%C3%B3nico.pdf.

205 / DEPA Art. 6.4, Acuerdo Art. 9.

206 / DEPA Art. 5.1 y 5.2, Acuerdo Art. 6.6.

207 / DEPA Art. 5.1, Acuerdo Art. 12.(f).

208 / Acuerdo Art. 6.7.

209 / DEPA Art. 4.2.8, 4.2.9 y 4.2.10.

210 / Acuerdo, Art. 10 y su nota. Esto es concordante con la legislación argentina.

211 / DEPA, Art. 6.2.

212 / Patrícia Varejão, "El aplazamiento de la firma del tratado entre Mercosur y Singapur", https://www.memo.com.ar/economia/el-aplazamiento-de-la-firma-del-tratado-entre-mercosur-y-singapur/

213 / Biblioteca de Chile, Tratado Integral y Progresista de Asociación Transpacífico (CPTPP), en https://www.camara.cl/verDoc.aspx?prmTIPO=DOCUMENTOCOMUNICACIONCUENTA&prmID=79273

214 / Véase el texto en español en http://www.sice.oas.org/Trade/TPP/CPTPP/Spanish/CPTPP_Text_s.pdf y http://www.sice.oas.org/Trade/TPP/Final_Texts/Spanish/Chapter14_s.pdf

215 / Véase Vera Thorstensen and Valentina Delich, "Convergence on e-commerce: the case of Argentina, Brazil and MERCOSUR", en Maarten Smeets, Adapting to the digital trade era: challenges and opportunities (2021), p. 246, disponible en https://www.wto.org/english/res_e/booksp_e/adtera_e.pdf.

216 / Una experiencia similar sucedió en países asiáticos, en los que el texto del CPTPP también se "exportó" casi textualmente a acuerdos bilaterales de comercio, tales como el Regional Comprehensive Economic Partnership ("RCEP") entre Australia, Brunei, Cambodia, China, Indonesia, Japon, Laos, Malasia, Myanmar, Nueva Zelanda, Filipinas, Singapur, Corea del Sur, Tailandia y Vietnam. Véase Kati Suominen, "Two Years into CPTPP" (Agosto 2021), en https://www.csis.org/analysis/two-years-cptpp.

217 / Jane Kelsey, "DEPA Lacks Added Value", en https://www.eastasiaforum.org/2020/04/10/depa-lacks-added-value

9. Autoría

Celia Lerman es abogada y socia en Lerman & Szlak, donde lidera el departamento de Propiedad Intelectual y el diseño y ejecución de estrategias de PI y privacidad transnacionales. Es codirectora de la carrera de Abogacía en UTDT, y miembro fundadora de ALAP (Asociación Latinoamericana de Privacidad).

Gabriela Szlak es abogada y socia en Lerman & Szlak, liderando el asesoramiento en Negocios Digitales, Comercio Electrónico, Privacidad y Propiedad Intelectual con foco en empresas del sector tecnológico. Es Consultora del Banco Mundial y profesora de Aspectos Legales y Regulatorios de los Negocios Digitales en maestrías de la Universidad de Buenos Aires.

Lucia Suyai Mendiberri es abogada graduada por UdeSA. Se especializa en Propiedad Intelectual, Tecnología y Protección de Datos Personales. Completó el Programa de Formación en Derecho de Internet y Tecnología de las Comunicaciones de UdeSA y actualmente se encuentra cursando la Maestría en Derecho y Economía en la UTDT.

adc.org.ar