Maestría en Derecho Empresario - UADE

Atomización en materia de transferencias internacionales de datos personales. ¿Regionalización o continuidad?

Maestranda: Natalia Lamarfa Sinisi.

Tutor: Silvia Susana Toscano

Contenido

I- INTRODUCCIÓN

Durante los últimos años, la transferencia internacional de datos personales ha adquirido una relevancia creciente en el campo de la privacidad y la protección de datos. Resulta entonces pertinente abordar dicha problemática desde la perspectiva del cumplimiento de datos, con el propósito de analizar los flujos internacionales de información y las vías mediante las cuales se concretan las transferencias, a fin de identificar posibles soluciones jurídicas y operativas que garanticen su adecuada gestión en distintos contextos de prestación de servicios.

La materia de transferencias internacionales resulta no sólo compleja e interesante, sino también extensa y de difícil abordaje debido a la atomización de su contenido. La existencia de múltiples cuerpos normativos relativos a naciones en particular toma notoriedad, ya que deben ser considerados en su contexto si se quisiera ejecutar cualquier tipo de servicio cuya transferencia de datos pueda tener raigambre de una manera global. Como se desarrollará a lo largo de esta presentación, analizar este tópico resulta de fundamental relevancia para una Maestría de Derecho Empresario, dado que examinar una potencial armonización legislativa en materia de transferencias internacionales de datos personales no solo fortalecería la seguridad jurídica desde un punto de vista exegético normativo, sino que también se constituiría como un factor clave para la estabilidad y previsibilidad que requiere la realización de negocios varios y diversos en un entorno globalizado y altamente tecnológico.

Hoy en día, la negociación contractual se configura de la siguiente manera: se establecen, o no, cláusulas de responsabilidad, se fija un término, se habla de indemnidad, se acuerdan pautas claras, y se entienden los límites negociables. Ahora bien, contando con una cantidad innumerable (en crecimiento) de ordenamientos jurídicos vigentes en materia de datos personales, hoy en día resulta una columna fundamental de discusión, no sólo respecto a la decisión sobre qué tipo de legislación aplicar, sino que también para comprender qué tipo de documentación requiere la ley aplicable, considerando qué se define como dato personal, y qué protección legal merece. Y no sólo hablamos de datos personales sensibles, al considerar que existen normativas que ya consideran a la data "*Business to Business*" o de contacto, como dato personal digno de protección[1].

[1] Véase el caso de *California Privacy Rights Act* no extendiendo la exención fijada por *California Consumer Privacy Act* (https://iapp.org/resources/topics/ccpa-and-cpra/).-

Las transferencias de datos personales se han vuelto, entonces, un tema central, y cabe sostener que se encuentra infravalorado a nivel de tratamiento legislativo.

Pese a que se encuentra en agenda parlamentaria, aún los debates no han logrado brindar una respuesta efectiva de regulación, que alcance los efectos y consecuencias de la realidad, debido a su dilatación en el tratamiento legislativo en distintas naciones y entidades.

Se realiza esta tesis avocada a las transferencias internacionales de datos personales, por creerse que la mayoría de las diferentes legislaciones emitidas en esta materia, han ido surgiendo de manera focalizada, cada normativa pensando en su propia realidad, sin dimensionar efectivamente la cantidad y naturaleza global e interrelacionada de las transferencias que ocurren de manera diaria y constante.

Lo antedicho, partiendo desde el mero acceso remoto a datos personales, visualizando un monitor compartido en una videollamada donde haya información pseudonimizada, o hasta inclusive guardando cierta información en una nube cuyo servidor esta geolocalizado en una ubicación remotamente distante a nuestra base presencial.

Resulta difícil dimensionar el impacto que la globalización y el avance tecnológico han generado en las transferencias internacionales de datos personales, entendidas conforme al Reglamento General de Protección de Datos (en adelante el RGPD o "*GDPR"*[2] por sus siglas en inglés). Podría decirse que inclusive dentro de los estándares comerciales este es el caso, amplificado ante la efectiva inserción de la inteligencia artificial en el procesamiento de datos, momento donde surge evidente que inclusive se debe verificar la posibilidad de procesar datos personales públicamente disponibles, dependiendo la legislación que resulte aplicable sobre los mismos. Servidores, terceros involucrados como *Sub-processors* en términos del RGPD, con evaluaciones de impacto de protección de datos (*DPIA, Data Protection Impact Assessment*) cada vez más complejas, resultan situaciones clave para disparar la necesidad de debatir y profundizar en este tema.

En este contexto, la elección del tema resulta clave para entender los negocios inmersos en la coyuntura vigente, su impacto en contexto y el abordaje jurídico efectivo necesario, así como las contingencias esperables en vista de lo que acontece en la práctica.

La protección de datos personales, y particularmente la transferencia internacional de los mismos, se ha convertido en un componente crítico y usual dentro del entramado jurídico que

[2] Versión actualizada disponible en https://gdpr-info.eu/

regula las relaciones comerciales globales, más aún con el surgimiento de nuevas tecnologías, difícilmente alcanzables de antemano desde el punto de vista legal por lo impredecible que resulta la configuración de nuevos mecanismos de transferencia.

Inicialmente podría observarse que la falta de armonización legislativa no sólo dificulta el cumplimiento normativo, sino que introduce un nivel de inseguridad jurídica que puede incidir directamente en la viabilidad de operaciones transfronterizas, elevando los costos legales, dilatando tiempos de implementación y afectando la predictibilidad que exige cualquier modelo de negocio viable.

Así entonces, cabe repensar la vigencia empírica de los marcos regulatorios, considerando si fuera pertinente incluirlos en una perspectiva regional y coordinada, o global inclusive, no sólo constituyendo una inquietud técnica, sino también una necesidad concreta para facilitar el comercio internacional en un entorno digital como el que actualmente se posee, tal como se demostrará a lo largo del presente trabajo.

La relevancia empresarial del tema, entonces, es incuestionable: en un mundo donde las transacciones y la prestación de servicios, sea cual fuera su fuero, materia y alcance, involucran flujos de datos constantes entre jurisdicciones adecuadas y no adecuadas, es fundamental contar con criterios jurídicos estables y previsibles para consolidar relaciones contractuales eficaces, brindando un marco de certeza a las partes involucradas. Así, este análisis identifica su objetivo principal en analizar, desde un punto de vista jurídico, siempre observando el impacto directo en los negocios, cómo el marco regulatorio, en este caso de protección de datos personales, puede, y debe, ser optimizado para ofrecer mayor seguridad jurídica a las partes contratantes, preservando los derechos de los titulares de datos personales, siendo el bien jurídico tutelado final.

Desde la práctica, resulta evidente la creciente interdependencia e interacción entre las economías a nivel global, respondiendo a una demanda de mercado que no retrocede en su entrelace a medida que pasa el tiempo. Aristas múltiples de análisis son posibles. Sin embargo, esta tesis de maestría se enfocará en indagar sobre la posibilidad de simplificar este paradigma, históricamente nuevo, que las transferencias internacionales de datos personales traen desde el área técnica e interdisciplinariamente acaban por desafiar al área jurídica, a intentar detectar riesgos para los cuales el legislador no se encontraba previamente preparado, sin por ello generar inseguridad jurídica por regular en diferentes países, operaciones casi instantáneas. Se

persigue cubrir vetas teóricas y prácticas, analizando la posibilidad, y conveniencia, de armonizar regulaciones de manera global.

II- **MARCO TEÓRICO – PERSPECTIVA SELECCIONADA.**

Durante la realización del análisis preliminar al presente trabajo, se indagó en el método óptimo para abordar el objetivo principal. Preguntarse si es posible uniformizar las legislaciones, y de ser así, si hacerlo es tomar la posición óptima que solucione esta situación. Comprendiendo que el hecho de tener una instancia de aplicación judicial (las cortes o autoridades respectivas que resulten designadas como competente por la legislación aplicable), no permite con ejemplos concretos en materia de datos personales pensar en un único ente jurisdiccional como entidad óptima revisora y de aplicación en términos judiciales, derivó en un análisis profundo de la materia. Es pertinente recordar instancias en las que la Corte "*permitía entusiasmarse con avances en materia de privacidad y derecho de protección de datos personales*"[3], como menciona Segura al abordar "Rodríguez c. Google", un fallo significativo en la materia. Cabe entender que la necesidad de ampliar la aplicación territorial de un cuerpo normativo tiene riesgos principales. La concentración de poder en un único ente con una mínima cantidad de expertos al mando podría ser una de las dificultades. Más aún, concentrado fuere el poder, las particularidades territoriales de cada jurisdicción quedarían subsumidas al escaso conocimiento que sólo una mínima cantidad de personas poseen sobre sus propios territorios, mas no sobre la realidad económico social de los territorios involucrados en el negocio del que se trate.

En este sentido, las premisas teóricas aquí expuestas constituyen el punto de partida del presente trabajo, reconociendo que se trata de una materia en plena evolución normativa y doctrinaria. Dada la reciente formulación de muchos de los criterios en análisis, el enfoque adoptado se basará en el examen de fuentes y textos actualizados, con el fin de ofrecer una interpretación contemporánea y consistente del estado actual del derecho comparado en materia de protección de datos personales.

[3] Segura, P. (2019) A un año de Rodríguez contra Google: ¿Estableció la CSJN un derecho al olvido digital en Argentina? – SAIJ - Recuperado de: https://www.saij.gob.ar/pablo-segura-ano-rodriguez-contra-google-establecio-csjn-derecho-al-olvido-digital-argentina-dacf150827/123456789-0abc-defg7280-51fcanirtcod?f=Total%7CFecha%7CEstado+de+Vigencia%5B5%2C1%5D%7CTema%2FDerecho+constitucional%5B3%2C1%5%20n%5B5%2C1%5D%7CTribunal%5B5%2C1%5D%7CPublicaci%20n%5B5%2C1%5D%7CColecci%20n+tem%20tica%5B5%2C1%5D%7CTipo+de+Documento%2FDoctrina&o=1&t=2797

Para entender las referencias claves de la presente tesis, parto de los principios en materia de procesamiento de datos personales contenido en el RGPD. La intención es utilizar al RGPD como referencia central para analizar la viabilidad de la armonización de distintos modelos y legislaciones que han ido adaptándose a lo largo del tiempo, inspirados en él o creados independientemente.

Por su parte, al referir a un territorio adecuado, estamos hablando de la terminología utilizada en el artículo 45 del RGPD, donde la Comisión Europea[4] como autoridad de aplicación, define la posición de un país como adecuado[5] siempre que considera a ese país que es un "tercero", fuera del espacio económico europeo (EEE, o *EEA* o *European Economic Area* por sus siglas en inglés, contemplando la Unión Europea, Noruega, Islandia y Liechtenstein), como poseedor de un nivel apropiado de salvaguardas legales, considerado equivalente en estándares al RGPD. Esta adecuación aludida, se basa en una concepción juzgada como "esencialmente equivalente" o con "protección equivalente", siguiendo a Kuner[6], al decir que esta comparación entre los estándares de protección de datos de un país tercero y los de la Unión Europea resulta sumamente complejo, ya que la protección de datos y la privacidad están profundamente ligadas al contexto cultural y social de cada país, lo que dificulta cualquier análisis comparativo directo, a lo cual se torna difícil generar una comparativa exacta. En este contexto, resulta indispensable reconocer que la protección de datos personales trasciende las fronteras normativas europeas y se proyecta sobre un ecosistema global interconectado.

Por ello, se parte aquí del presupuesto en que la interoperabilidad y la internacionalidad con la que las transferencias de datos en general, no solamente personales, se realizan a diario y por ello se requiere una atención no sólo local, sino tendiente a que posea una coherencia global. Para ello, se utilizará el término armonización, pensando en él como un proceso mediante el cual se ajustan y coordinan normas jurídicas de distintos sistemas legales, persiguiendo compatibilizarlas, mantenerlas cohesivas y hasta inclusive uniformes en determinadas materias, teniendo como principio rector la necesidad de seguir respetando las particularidades nacionales.

[4] *European Commission* página oficial https://commission.europa.eu/protection-your-personal-data_es
[5] Lista actual: Andorra, Argentina, Canada (para organizaciones comerciales) Islas Feroe, Guernesey, Israel, Isla de Man apón, Jersey, Nueva Zelanda, República de Corea, Suiza, el Reino Unido, los Estados Unidos (sólo en organizaciones comerciales que participan en el Marco de Privacidad de Datos UE-EE. UU.) y Uruguay.
[6] KUNER, C. (2017) "Reality and Illusion in EU Data Transfer Regulation Post Schrems" German Law Journal, Volume 18, Issue 4, 01 July 2017, pp. 881 – 918 DOI: https://doi.org/10.1017/S2071832200022197 - Recuperado de https://www.cambridge.org/core/journals/german-law-journal/article/reality-and-illusion-in-eu-data-transfer-regulation-post-schrems/0341A0D14DC345730F9B48A496A968D3

Teniendo en cuenta la complejidad del modo hacia donde están fluctuando las transferencias internacionales de datos personales, es cada vez más necesaria la utilización de cláusulas estándares si se quiere realizar procesamiento, acceso, colección de datos y cualquier otro tipo de acción, en el marco de lo previsto por ley. A lo cual, los términos referidos a normativa de privacidad propiamente dicha (tales como datos personales, responsable (o *controller*), encargado (o *processor*), procesamiento, *standard contractual clauses* / cláusulas contractuales estándar (en adelante "SCC", CCE, Cláusulas estándar, Cláusulas modelo, *Standard Contractual Clauses*, Cláusulas Contractuales Estándar, utilizadas de manera indistinta evitando repetición innecesaria, destacando y difiriendo entre ellas cuando sea necesario), tendrán la acepción dada a las mismas en el RGPD, salvo que se indique expresamente lo contrario.

En este marco, comprender la evolución de los instrumentos jurídicos que buscan materializar esta armonización resulta esencial. La teoría sobre la coherencia global en materia de privacidad encuentra su correlato práctico en los mecanismos de transferencia internacional de datos, diseñados precisamente para compatibilizar sistemas legales heterogéneos bajo criterios de equivalencia sustancial. Así, las SCC emergen como una respuesta concreta al desafío de garantizar niveles de protección uniformes más allá de las fronteras europeas, constituyéndose en uno de los pilares fundamentales del sistema global de cumplimiento en materia de protección de datos.

Indagando en esta última cuestión, los antecedentes que dieron origen a las SCC, desde la perspectiva de Corrales Compagnucci[7] y su equipo, tienen su génesis en los fallos Schrems I (2015)[8] y Schrems II[9] (2020) del Tribunal de Justicia de la Unión Europea, que declararon inválidos los mecanismos previos de transferencia de datos entre la Unión Europea y Estados Unidos, el *Safe Harbour*, acuerdo que pactaba un tratamiento para que los datos personales puedan transferirse legalmente entre un Estado Miembro de la Unión Europea y Estados

[7] Corrales Compagnucci, M., Aboy, M., & Minssen, T. (2021). *Cross-Border Transfers of Personal Data After Schrems II: Supplementary Measures and new Standard Contractual Clauses (SCC).* Nordic Journal of European Law, 4, Article 2. Recuperado de: https://doi.org/10.36969/njel.v4i2.23780

[8] CJEU, C-362/14 "Schrems I"; European Commission Implementing Decision (EU) 2021/914. Abordado en EUROPEAN PARLIAMENT A" Exchanges of Personal data After the Schrems II Judgment." Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 694.678 – Recuperado de https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

[9] CJEU, C-311/18 "Schrems II""; European Commission Implementing Decision (EU) 2021/914. Abordado en EUROPEAN PARLIAMENT A" Exchanges of Personal data After the Schrems II Judgment." Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 694.678 – Recuperado de https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

Unidos, con fines comerciales, a través de "*un sistema de auto certificación*"[10], y posteriormente el *Privacy Shield*, siguiendo a Ortega Giménez[11], un nuevo mecanismo que destacaba salvaguardias claras con obligaciones de transparencia en cuando al acceso por parte de la administración estatal, por no garantizar un nivel de protección equivalente al exigido por el RGPD frente a las prácticas de vigilancia masiva estadounidenses.

Como consecuencia de dichas decisiones, las SCC pasaron a consolidarse como la herramienta principal para legitimar las transferencias internacionales de datos personales, complementadas desde 2021 con nuevas versiones adoptadas por la Comisión Europea que introducen un enfoque modular, mayores obligaciones de evaluación de impacto y medidas técnicas adicionales para asegurar la equivalencia sustancial del nivel de protección[12]. Con intentos posteriores como el *Data Privacy Framework,* en adelante "DPF" indistintamente desde aquí, siguiendo nuevamente a Ortega Giménez[13], un nuevo marco que impuso la limitación del acceso por parte de los servicios de inteligencia estatales, y un tribunal de recurso en materia de protección de datos para ciudadanos, se intentan proteger las transferencias entre Estados Unidos y la Unión Europea, comenzando a evidenciarse una doble dimensión.

Por un lado, la necesidad de generar una vía facilitadora para la realización de transferencias seguras, no pudiendo garantizar la libre circulación del capital económico en las diferentes industrias, ya que, en una gran proporción de estas, ciertos datos personales, en mayor o menor grado de sensibilidad y cuantía, acaban siendo intercambiados. Pero a su vez, en segundo lugar, se evidencia una complejidad en la determinación del marco aplicado, a lo cual el DPF como solución prevé una solución que aparentaría priorizar el principio de economía procesal, al poner en cabeza del *processor* la obligación de "auto certificarse", parafraseando a Lönnberg[14], vía el uso de un programa administrado por el Departamento de Comercio de los Estados

[10] Sobrino García, I. (2021). Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y Estados Unidos. Revista de Derecho Comunitario Europeo, 68, 227-256.

[11] Ortega Giménez, A. (2017). Transferencia internacional de datos personales: del Safe Harbour al Privacy Shield. RLM nº4. Artículo nº 12. Páginas 85-90. Recuperado de: revistalexmercatoria.umh.es

[12] CJEU, C-362/14 "Schrems I"; C-311/18 "Schrems II"; European Commission Implementing Decision (EU) 2021/914.

[13] Ortega Giménez, A. (2024). ¿Y a la tercera va la vencida?... El nuevo marco transatlántico de privacidad de datos UE-EE. UU. Cuadernos de Derecho Transnacional (marzo 2024), Vol. 16, Nº 1, pp. 483-513.

[14] LÖNNBERG, C. (2025) "Compliance Risks for EU Controllers The DPF Disproportionate Burden-Expense Exception and its Effects on EU Controllers' Duty to Provide a Copy of Personal Data via U.S. Processors" Tesis de Graduación – Master of Laws Program – Lund University. Recuperado de: https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9189189&fileOId=9197588 – pp. 25 - Texto en idioma original, parafraseo con traducción propia*: "U.S. companies can self-certify to the DPF through a program administered by the U.S. Department of Commerce. Once certified, a company is deemed an authorized data recipient under EU law, and transfers to it from the EU can take place freely"*

Unidos, donde una vez certificada, la compañía estadounidense que aplicaría al DPF luego de pasar por un proceso de aprobación administrativo, pasa a ser entendida como un receptor autorizado bajo las leyes de la Unión Europea en materia de privacidad de datos.

A partir de estas experiencias recientes, resulta evidente que los esfuerzos aislados, aunque valiosos, no alcanzan por sí solos para resolver la fragmentación existente. De allí surge la necesidad de avanzar hacia un proceso de armonización legislativa que otorgue coherencia y estabilidad al régimen de transferencias internacionales de datos personales.

Cabe empezar señalando que la armonización legislativa en materia de transferencias internacionales de datos personales constituye como un factor clave para las empresas que operan en un entorno globalizado, es decir, todas sin excepción alguna. No sólo porque a dichas empresas se les aplique ese marco normativo, sino también para que logren simplemente dirimir si existe o no procesamiento que requiera una salvaguarda adicional, de una manera directa y precisa.

Actualmente, la coexistencia de múltiples marcos regulatorios, con sus diferencias y especificidades, genera una nebulosa de incertidumbre y amplios costos adicionales, difícilmente mesurables de antemano. En primer lugar, el costo de entender qué regulaciones acaban siendo aplicables, para sobre ello discutir la estructuración de contratos alrededor de la ley aplicable y sus requisitos, y finalmente orientar esfuerzos a medir, dimensionar y administrar de riesgos legales de forma integral.

El presente trabajo parte del supuesto que un esquema armonizado permitiría a las empresas reducir la complejidad operativa y jurídica, así como el personal propio y tercerizado necesario para llevar a cabo una transferencia legítima en estos términos.

Además, contar con variables claras permite optimizar procesos, agilizando la toma de decisiones y facilitando la expansión del negocio de cada entidad a nuevos mercados, pudiendo previsualizar cuáles son las medidas adicionales que deberían tomar en caso de expandirse hacia una u otra geografía. La seguridad jurídica resultante de un esquema que permita previsibilidad y sea predecible sobre su aplicación, y hasta sobre sus sanciones, no sólo protege los derechos de los titulares de datos, sino que también invita al conglomerado empresarial a participar en un ambiente más competitivo y confiable para la inversión internacional, utilización y aprovechamiento de nuevas tecnologías emergentes, que terminan traduciéndose en innovación empresarial.

Esta fragmentación y división normativa representa un desafío para los actores involucrados, ya que incrementa la incertidumbre y complejidad jurídica en la planificación y ejecución de cualquier negocio que involucre transferencia de datos personales internacionales.

La ausencia de un marco jurídico armonizado obstaculiza el cumplimiento eficiente y genera un incremento de los costos legales para las partes contratantes, con impacto negativo en la competitividad empresarial. Avanzar hacia una mayor coherencia normativa no solo es una cuestión técnica, sino una necesidad empresarial estratégica, para fortalecer la seguridad jurídica, brindar certeza a las partes involucradas y consolidar un entorno favorable para el desarrollo y la innovación empresarial en un contexto globalizado y digital como el que se habita en el Siglo XXI.

Huelga aclarar que, dado el carácter emergente y dinámico del régimen jurídico aplicable a las transferencias internacionales de datos personales, parte del análisis desarrollado en esta tesis se sustenta en fuentes primarias actualizadas al año 2025, incluyendo textos normativos, decisiones administrativas y proyectos legislativos recientes. Ello obedece a que, por la novedad del tópico, aún no existen estudios doctrinarios o jurisprudenciales exhaustivos que aborden integralmente las cuestiones tratadas.

En consecuencia, en ciertos casos se recurre al examen directo de la norma y de documentos técnicos emitidos por autoridades competentes, procurando mantener la rigurosidad metodológica y la coherencia conceptual propias de un trabajo de investigación jurídica de esta índole.

Será uno de los objetivos analizar la posibilidad normativa de equilibrar las tensiones entre las necesidades que los nuevos fenómenos prácticos en el área de privacidad posicionan, contra la posibilidad jurídica de cubrir esos nuevos requerimientos, ponderando las herramientas que hoy en día posee.

III- METODOLOGÍA – VARIABLES EN ANÁLISIS.

i. Variables

V.1: Armonizar y concentrar los mecanismos de protección para la transferencia internacional de datos personales.

La acción bajo análisis es la variable independiente. Armonizar los mecanismos en un único documento. Habrá diferentes condiciones por las cuales pueda o no llevarse a cabo debidamente.

V.2: Una regulación en proceso de consolidación.

La variable dependiente, ya que sujeto al prematuro estado de esta legislación, no podría llevarse a cabo exitosamente una uniformización de la legislación en materia de transferencia internacional de protección de datos.

A nivel relación entre variables, podría decirse que la posibilidad de ejecutar exitosamente la premisa establecida en la variable independiente se encuentra sujeta al estado de maduración que posea la utilización de cláusulas contractuales estándares de diferentes regiones.

ii. Objetivos

a. Objetivo General

Se persigue con el presente trabajo de tesis, analizar la viabilidad jurídica y práctica de la regionalización de las normas sobre transferencia internacional de datos personales como alternativa frente a la imposibilidad actual de lograr una armonización global efectiva.

b. Objetivos Específicos

1) Identificar los principales marcos normativos internacionales en materia de protección de datos personales y sus divergencias.
2) Examinar los factores jurídicos, institucionales y económicos que dificultan la armonización global.
3) Evaluar los avances y limitaciones de los procesos regionales de integración en la materia (UE, Mercosur, ASEAN, entre otros).
4) Proponer lineamientos que contribuyan al desarrollo de un marco regional coherente que facilite la seguridad jurídica y la expansión empresarial en el entorno digital.

IV- HIPÓTESIS BAJO ANÁLISIS

Armonizar globalmente las normas sobre transferencia internacional de datos personales resulta inviable en la actualidad, dada la disparidad de marcos regulatorios y la ausencia de

organismos supranacionales con potestad vinculante. Sin embargo, la regionalización normativa través de bloques de integración como la Unión Europea, el Mercosur o la Asociación de Naciones del Sudeste Asiático (ASEAN), constituye una alternativa viable y estratégica para reducir la fragmentación jurídica, fortalecer la seguridad en las transacciones internacionales y promover la competitividad empresarial en un entorno digital globalizado.

V- DESARROLLO

i. Naturaleza de la vinculación

A los fines de ceñir el análisis a casuística en particular, se limitará el análisis a la examinación de la eficiencia del método existente disponible en vías de celebración de un contrato, cuyo alcance de servicio pueda involucrar transferencia de datos personales internacionalmente. Lo antedicho, deviniendo en la necesidad de sumar a las bases contractuales de índole comercial, anexos específicos que logren cubrir la demanda desde un punto de vista de *Data Compliance*.

Las SCC se definen como un contrato entre partes. A diferencia de lo que usualmente ocurre con los *Data Processing Agreement* (o "DPA" indistintamente utilizado), que solamente siguen los lineamientos establecidos en el artículo 28 del RGPD, dejando a libertad de las partes el cómo volcar su contenido, las SCC configuran disposiciones oficialmente estandarizadas y aprobadas por la jurisdicción en la cual fueron emitidas. En general, estas cláusulas resultan invariables, y su nombre puede ir variando respecto a la legislación aplicable.

Respecto a su naturaleza y aplicación, puede decirse que son parte de un contrato accesorio, anexando a un principal cuya relación jurídica fundamental es un negocio o acto jurídico patrimonial desarrollado entre las partes.

Específicamente al estar negociando un DPA, parafraseando a Kwiatkowska[15], el *controller* es responsable de asegurar que las transferencias de datos a jurisdicciones distintas de aquellas donde fueron recolectados se realicen en cumplimiento de las normativas aplicables. Pese a la

[15] KWIATKOWSKA, M (2019) *"Negotiating a data processing agreement: a practical perspective"* – Derecom: Revista Internacional de Derecho de la Comunicación y las Nuevas Tecnologías, ISSN-e 1988-2629, Nº. 27 – Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=7064843 - pp. 184 – Traducción propia.

existencia de mecanismos específicos existentes al momento, la autora persiste sosteniendo que las partes deben contemplar métodos alternativos de solución en caso de encontrarse fuera de cumplimiento con la normativa vigente, brindando como alternativas que se detendrá el procesamiento y se dará por terminado el contrato, o el encargado garantizará otro mecanismo legal para continuar las transferencias, para finalmente poder prever que ambas partes cooperarán de buena fe para encontrar una solución conjunta.

A saber, cuando desde una perspectiva de negocio se quiere llevar a cabo un servicio que acaba por involucrar el procesamiento de datos personales en un país diferente al lugar en donde se originaron los datos, o el responsable del tratamiento está basado en un país y los datos van a transferirse hacia otro país, o finalmente el titular de datos personales (dependiendo qué tipo de normativa aplique podría hablarse de residente, *householder*[16], consumidor, entre otras categorías) posee y provee datos en un país que luego serán procesados en otro.

El acto de "procesar" abarca un espectro muy amplio de posibles accionares. Desde el mero acceso remoto visualizando una pantalla compartida, conteniendo datos personales para prestar el servicio para el cual se contrató al encargado de tratamiento, hasta almacenar en un servidor o colectar datos específicamente, cada vez más y más acciones de la vida comercial requieren transferencias, y por la globalización en sí es cada vez más difícil garantizar que los datos personales se queden estancados en un territorio en particular.

La excepción a la aplicación de las SCC cuando hay una transferencia internacional de datos personales, está dada en el caso de los países adecuados, donde se puede circular libremente, siempre que se posea el consentimiento apropiado y se garanticen los principios básicos en materia de derecho de privacidad de datos, como si fuera dentro de los límites nacionales. Recordemos que, desde la perspectiva de Phillips[17], dicha adecuación exige que las transferencias se realicen mediante un mecanismo previamente aprobado por una autoridad, que garantice un nivel de protección aceptable en la jurisdicción de destino. En contraposición, cuando la transferencia no se realiza hacia un país considerado adecuado, cobran especial relevancia las SCC, que actúan como el principal instrumento jurídico para garantizar la licitud y seguridad de dichas operaciones internacionales.

[16] CCPA actualizada por CPRA.

[17] PHILLIPS, M (2018) *"International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)"* Hum Genet , 575–582 (2018). https://doi.org/10.1007/s00439-018-1919-7 - Recuperado de: https://link.springer.com/article/10.1007/s00439-018-1919-7#citeas – pp. 576 – Traducción propia.

El hecho que estas cláusulas sean estándar facilita su aplicación, negociación y entendimiento, si se lo contrasta con lo que acontece con los DPA. Lo antedicho, ya que constituyen un contrato en particular sujeto a negociación de las partes, discusión acerca del *template* a utilizar, así como numerosos costos acarreados consigo como la contratación de personal especializado, necesidad de involucrar áreas operativas por el contenido que este tipo de negociación involucra, y demás vicisitudes devenidas de una propia negociación.

Puede confirmarse entonces que las SCC como instrumento facilitan la transferencia de datos personales a nivel internacional garantizando el cumplimiento normativo. Sin embargo, su complejidad al momento de utilizarlas se evidencia y toma relevancia a nivel global, cuando una transferencia involucra múltiples países como exportadores de los datos personales, donde no se identifica un cuerpo único de SCC aplicable, sino que distintas SCC, bajo distintas denominaciones, se encuentran segregadas a lo largo del mundo, cada país emitiendo la suya, a excepción del caso de las regionalizaciones como el caso del EEE, donde todos los países parte, gozan de los beneficios de poseer las mismas SCC.

En consecuencia, si bien las SCC representan un instrumento esencial para viabilizar las transferencias internacionales de datos personales dentro de un marco jurídico seguro, su implementación práctica continúa planteando interrogantes relevantes. La heterogeneidad de sus versiones en diferentes países y la ausencia de un cuerpo unificado a nivel global invitan a reflexionar sobre sus alcances reales y sobre los desafíos que su aplicación conlleva en distintos contextos normativos.

ii. **Ponderación de las SCC**

Podría decirse que la implementación de SCC tiene ventajas y desventajas, como toda solución legislativa que se pueda tomar para regular una cierta situación.

Respecto a los beneficios, cabe señalar que, al poseer un borrador estandarizado e invariable, los tiempos de negociación se reducen, como se previno en el acápite anterior. Sin embargo, la problemática principal del carácter difuso de la jurisdicción sobre el dictado y contenido de las SCC se alinea a los altos costos de implementación, principalmente a nivel económico y temporal.

Ya a nivel general, en materia de privacidad de datos, doctrinarios tales como Chander[18] y su equipo, ya a principios de la década que corre, comenzaron a identificar la amplia variedad de costos que puede acarrear consigo la puesta en práctica de medidas apropiadas en materia de privacidad de datos. En ese sentido, los autores sostienen que el costo de cumplir con las leyes de privacidad varía enormemente, dependiendo si se trata de una panadería que gestiona una pequeña base de datos con los pedidos de sus clientes habituales, llegando a la dimensión de una empresa de mil empleados que presta servicios de información a distintos clientes en múltiples jurisdicciones Esta disparidad en los costos de cumplimiento no sólo refleja la complejidad técnica del marco regulatorio, sino que también pone de manifiesto las dificultades económicas y operativas que enfrentan las organizaciones al intentar adecuarse a múltiples regímenes legales simultáneamente.

En este sentido, resulta menester destacar que económicamente, la necesidad de contar con un cuerpo letrado especializado no sólo en la materia de protección de datos, sino también involucrado en la actualidad de todas las legislaciones vigentes a nivel mundial, complejiza la implementación adecuada con recursos limitados.

Aquí no sólo se hace referencia a las transferencias donde una empresa voluntariamente coloca ese dato personal, sino también las situaciones donde se opera como encargados del tratamiento, y el correspondiente subencargado (entendiendo aquí al *processor* o encargado del tratamiento involucrado por otro encargado previamente, "*subprocessor"* o subencargado indistintamente desde aquí) decidió relocalizar su servidor (base de datos) hacia un país no adecuado, debiendo inmediatamente poseer los recursos y capacidades de revisión jurídica necesarios para poder analizar el cuerpo normativo de cobertura propio del país en que se coloque ese servidor. En adición, es menester asegurarse de no tener una restricción territorial que imposibilite esta situación, derivada de una prohibición por parte de nuestro responsable.

Asimismo, hay un costo adicional, no precisamente ponderable, que tiene que ver con la celeridad con la que tal vez un cierto negocio venía desarrollándose, con términos casi estandarizados, mientras que a la luz de la nueva normativa deba comenzar a considerar un plexo en materia de transferencias internacionales de datos personales completamente nuevo,

[18] CHANDER, A. et Al (2021) "*Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation"*- Policy Research Working Paper 9594. World Bank's World Development Report 2021 Team in collaboration with the Macroeconomics, Trade and Investment Global Practice. Georgetown Law Faculty Publications and Other Works. 2374., Available at SSRN: https://ssrn.com/abstract=3827228 or http://dx.doi.org/10.2139/ssrn.3827228 Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827228 - pp. 9 – Traducción propia.

desconocido, y que, en consecuencia, genera resistencia. Más aún, si ese nuevo plexo normativo no es incorporado por referencia, sino incorporado en texto completo, puede inclusive acarrear consigo una sobrecarga hacia la contraparte (más si se trata de una PYME), quien vea un nuevo apéndice tal vez inclusive más largo que el propio contrato en sí, generando frustración intrínseca al momento de comenzar una negociación.

Sin embargo, la importancia de la puesta en lugar de las SCC acaba sobrepasando los intereses personales involucrados en cualquier negocio. Siendo el bien jurídico a tutelar la protección de los datos personales procesados de los titulares, ajenos al responsable y encargado del tratamiento, el debate pasa a extrapolar a las partes, y colocarlas en un lugar de meros gestores que deben preservar esos datos de la parte cuyos datos desean procesar a los fines de prestar cierto servicio ajeno al tercero.

iii. Adopción de las SCC

A medida que avanza el tiempo y se complejizan las transferencias de datos internacionales, el riesgo por no poseer SCC en su lugar, es cada vez mayor. Los estándares de las diferentes industrias se van adaptando, e inclusive para mantener ciertas certificaciones requeridas en el mercado (inclusive para beneficios fiscales), las cuestiones de privacidad de datos y seguridad de la información se vuelven cada vez más relevantes, y auditables inclusive.

El desafío de adaptación de las SCC se puede analizar desde diferentes perspectivas. Principalmente puede ser mencionada la adaptación a nivel estatal, cuyo desarrollo y grado de implementación varía según las capacidades normativas, institucionales y tecnológicas de cada país, tal como lo señalan Shi[19] y sus coautores. Su incoe y exigibilidad, así como también por otro lado, la adopción de las mismas por parte de los particulares, ya sea a nivel de la generación de un acuerdo nuevo donde deban incorporarlas como un tópico anexo adicional, o como también en la necesidad de revisar los acuerdos firmados previamente en donde aún se procesa datos personales, donde los periodos de transición e implementación tienen una fecha de

[19] SHI, P. et Al (2021) *"Governance of Privacy Protection: How Laws Will Be Adopted to Address New Technologies?"* 23rd Biennial Conference of the International Telecommunications Society (ITS): "Digital societies and industrial transformations: Policies, markets, and technologies in a post-Covid world", Online Conference / Gothenburg, Sweden – Recuperado de https://www.econstor.eu/handle/10419/238053

vencimiento, requiriendo sean adaptados para proteger los intereses de los sujetos cuyos datos se procesan, más aún, a nivel internacional.

Entre compañías, las SCC son el método más utilizado para proteger transferencias de datos personales a nivel internacional. Sin embargo, dentro del mismo grupo empresarial, las empresas tienen otras opciones para poder cubrir sus transferencias de manera legítima, sin necesidad de ingresar en una SCC diferente con cada una de sus entidades (ejemplos principales, las *binding corporate rules ("BCR")* (analizado exhaustivamente en escritos como el de Pietrzak[20]), como indica Maksó, establecidas como la institución jurídica más reciente destinada a garantizar salvaguardias adecuadas en los casos de transferencias internacionales de datos[21], o cualquier acuerdo *intra-company* con nivel suficiente de protección de datos que pueda realizarse). Lo antedicho, ya que las transferencias no sólo cubren las operaciones realizadas con terceros no afiliados, sino también con las propias entidades del mismo grupo, siempre que se encuentren ubicadas en un territorio ajeno a donde se originaron.

iv. Cláusulas estándar

Partiendo de la utilización de definiciones básicas, las SCC específicas de la jurisdicción donde se opere pueden ser aplicadas para cualquier transferencia de datos personales partiendo desde el país de origen hacia otro país que no sea considerado adecuado.

A nivel datos personales, y analizando su relevancia, podría partirse diciendo que la normativa faro que actualmente rige, resulta ser el RGPD, nucleando una gran cantidad de países adecuados que contemplan previsiones basadas en sus principios base.

A fin de facilitar el análisis que se propone, resulta esencial reconocer que la fragmentación normativa vigente genera un impacto directo en los costos y la eficiencia del cumplimiento regulatorio. Ello se traduce en la necesidad de contar con recursos especializados que abarquen de manera integral el diverso marco normativo aplicable a las transferencias internacionales de datos, para evaluar correctamente la aplicabilidad de la regulación en cada jurisdicción

[20] PIETRZAK, S. (2017) – "*TRANSBORDER DATA FLOWS: BINDING CORPORATE RULES AS A GLOBAL TRANSFER MECHANISM AND TRUSTED DATA PROCESSING AREA"* – Master Thesis Law and Technology LLM – Tilburg University – Recuperado de: https://arno.uvt.nl/show.cgi?fid=142708

[21] MAKSÓ, B. (2016). "*EXPORTING THE POLICY - INTERNATIONAL DATA TRANSFER AND THE ROLE OF BINDING CORPORATE RULES FOR ENSURING ADEQUATE SAFEGUARDS*." Pécs Journal of International and European Law, (II) – Recuperado de https://journals.lib.pte.hu/index.php/pjiel/article/view/6871

involucrada, así como poder dar lugar a la realización de evaluaciones diferenciadas en cada una de ellas, cuyos cuerpos normativos diferentes, en muchos casos no son comparables. Cada país involucrado en una transferencia compleja de datos personales, y la detección de su normativa aplicable, implica un considerable consumo de tiempo y esfuerzo.

En este escenario de creciente complejidad normativa y operativa, diversos autores han abordado el impacto práctico de dicha fragmentación sobre las organizaciones que operan globalmente, particularmente aquellas que dependen del almacenamiento y procesamiento en la nube. A lo largo del tiempo, las SCC han ido flexibilizando su contenido, contemplando nuevos roles, e incorporando nuevos escenarios. Sin embargo, el derecho acaba por ubicarse siempre tras los hechos, y hoy en día, si el responsable de tratamiento desea poner en lugar todas las SCC existentes porque realmente posee una operatoria global con sujetos y servidores ubicados en múltiples ubicaciones, se topa con la necesidad de combinar e incorporar al contrato principal, y al DPA, más de (al menos) diez cuerpos normativos diferentes, bajo la temática SCC.

En línea con esta dificultad práctica, Patterson[22] analiza cómo las transferencias internacionales de datos en entornos de nube enfrentan crecientes tensiones entre las regulaciones de privacidad estadounidenses y las exigencias de soberanía de datos de otras jurisdicciones, especialmente la Unión Europea y Asia. A partir de diversos casos empresariales, en este caso particular autor evidencia que la coexistencia de marcos como el RGPD generan conflictos normativos que obligan a las compañías globales a implementar estrategias híbridas, como la segmentación de datos, las SCC o el uso de servicios regionales de nube, para mantener la eficiencia operativa sin vulnerar las restricciones locales. De este modo, el autor enfatiza la necesidad urgente de una gobernanza global más armonizada, que permita equilibrar la protección de la privacidad con las demandas de competitividad y agilidad empresarial en un entorno digital interconectado.

Tomando como base estas reflexiones, resulta pertinente retomar la finalidad original de las SCC y su potencial para simplificar la operatoria global, sin desatender la protección efectiva de los titulares de datos. Como se señaló, la intención inicial de las SCC es tender a la máxima fluidez posible de los datos personales a nivel internacional, sin por eso generar inseguridad

[22] PATTERSON, T. (2025) *"Cross-Border Cloud Data Transfers: Case Studies on Balancing U.S. Government Privacy Regulations with Global Business Needs"* SSRN. Independiente http://dx.doi.org/10.2139/ssrn.5383863. Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5383863 - Traducción propia.

jurídica para ninguno de los sujetos de datos personales cuya información de esté procesando y transfiriendo en consecuencia.

Cabe preguntarse entonces, si de alguna manera resulta posible imaginar un panorama simplificado de las SCC, buscando ofrecer una mayor interoperabilidad entre diversas normativas, tornándolas comparables, a fin de reducir los costos de cumplimiento (pensando en que el negocio no está concentrando su operatoria sólo en esta área, sino que el DPA y las SCC son sólo una parte de la negociación), ayudando a que las empresas puedan operar globalmente con mayor facilidad, siempre que se sigan alineando con los principios fundamentales del RGPD.

v. Incentivos y régimen sancionatorio

En virtud de lo antedicho, y más allá de las previsiones teóricas bajo las cuales las SCC se dictan, este nuevo plexo acaba convirtiéndose en un paso adicional, administrativamente abrumante, para las unidades de negocios que procesen datos personales dentro de su operatoria cotidiana.

Como todo cambio, y más aún un cambio con el nivel de complejidad técnica que las SCC representan, genera resistencia y al efecto su implementación no ha sido uniforme y dócil como los fundamentos de estas aparentarían prevenir.

Para lograr la implementación masiva de las SCC, han tenido que acontecer diferentes penalidades a nivel global en materia de privacidad de datos en general, y sobre distintas compañías de gran renombre, con objetos de negocio completamente variados. Las conductas ejemplificadoras, acabaron siendo un motor para comenzar la oleada de implementación generalizada, principalmente entendiendo que la última actualización de las SCC es de 2021, y hay contratos con validez a 5, 10 años y *evergreen* (por tiempo indeterminado) que se encuentran vigentes desde momentos previos a su implementación.

Analizar qué tipo de sanciones se esperan si una parte procesa datos personales sin colocar las SCC en lugar, es menester en esta instancia.

Como principio, la falta de SCC se traduciría en la imposición de sanciones pecuniarias y patrimoniales por parte de las autoridades de control y aplicación. La intención en este caso es

disuadir prácticas que comprometan la seguridad y legalidad del tratamiento transfronterizo de datos, entendiendo al bien jurídico tutelado de fondo siendo la protección de los sujetos titulares de datos personales, para así poder reforzar la obligación de establecer garantías adecuadas para proteger dichos derechos en contexto de transferencias internacionales.

Ahora bien, excepciones a nivel pena en materia de protección de datos personales en general tendiendo a aplicaciones más duras, existen. El principal caso para mencionar es el de Corea del Sur. Allí, la legislación aplicable prevé posibles penas hasta cinco años de prisión o multa de hasta 50 millones de won por la transferencia de datos personales sin consentimiento[23], sin ceñirse en la enumeración de imposición potencial de penalidades sólo al EEE.

En el caso de *HIPAA*, *Health Insurance Portability and Accountability Act*[24], dentro de los Estados Unidos, país que al no poseer una normativa unificada en la materia no posee aún una tradición sólida de incorporación de protecciones específicas en materia de protección de datos personales, sólo considerando adecuado el DPF, si el encargado del tratamiento obtiene la certificación adecuada), reemplazando los intentos fallidos previos mencionados en el marco teórico, Schrems I y II, el *Privacy Shield* y el intento de *Safe Harbour*, ha aplicado sanciones económicas ejemplares que aunque no siendo un completo desincentivo, resultan al menos ejemplificadoras de los posibles costos a los que se puede enfrentar una unidad de negocios si evita aplicar las previsiones en materia de transferencia internacional de datos personales específicamente, y de datos personales en general.

A nivel normativa general, una multa podría llegar a comprometer hasta el tres (3) o cuatro (4) por ciento del valor total de facturación anual que la empresa involucrada lleve a cabo. Sin embargo, los casos citables con aplicación de procedimientos sancionatorios son pocos comparados a la cantidad de operaciones de procesamiento de datos sin cobertura de SCC detrás que se realizan a diario.

Es la falta de incentivos en severos regímenes legales, lo cual impulsaría a evitar la puesta en lugar de la cantidad de resguardos suficientes (distintas cláusulas estándares, modelo y/o con el nombre que posean) para encontrarse en cumplimiento con los requisitos de todos los países desde los cuales pudiera llegar a estarse procesando datos personales, derivando en una suerte

[23] REPUBLIC OF KOREA. (2023). PERSONAL INFORMATION PROTECTION ACT (ACT NO. 14839, AMENDED 2023). KOREA LEGISLATION RESEARCH INSTITUTE – Recuperado de: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=62389&lang=ENG

[24] Versión dictada por ley Ómnibus disponible en https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html

de salvataje por parte de quienes prestan servicios, prefiriendo aguardar una potencial sanción económica, a tener que abonar consultoría externa especializada en cada uno de los países involucrados. Lo antedicho, resulta más oneroso en términos no sólo de pago al estudio jurídico especializado en datos personales, sino también respecto a una posible dilación de la firma de contrato en base a la falta de acuerdo en la utilización de ciertas cláusulas contractuales y/o falta de recurso idóneo para revisar cada una de ellas por parte de la contraparte contratante, al menos a primera vista.

Pese a que la amenaza de multa existe, resulta pertinente el estudio realizado por Wolff[25] y su coautora, quienes analizaron 261 resoluciones de las autoridades europeas de protección de datos durante los dos primeros años de aplicación del RGPD, al revelar que la mayoría de las multas impuestas fueron de bajo monto y se concentraron en pocos artículos, principalmente vinculados a la protección de la privacidad del usuario, pueden sacarse ciertas conclusiones.

Las multas e infracciones por seguridad recibieron las sanciones más altas, pero, sin embargo, los distintos países demostraron haber aplicado el régimen de manera desigual, mostrando una implementación heterogénea y prudente del nuevo marco sancionatorio del RGPD. Más aún, considerando que en un análisis de 261 casos en dos años, una cifra mínima frente a la cantidad de transferencias internacionales que se realizan a diario impulsadas por el uso masivo de internet y la globalización, las multas pueden ser altas, pero la falta de casuística masivamente aplicada no parecería representar una amenaza inminente e inmediata para las unidades de negocio, como para llegar a considerarlas dentro de un presupuesto de costos o riesgos operacionales en el corto y mediano plazo.

Podría decirse entonces que prácticamente no existen incentivos para prevenir los incidentes ni el tratamiento inapropiado en materia de protección internacional de datos, y sí se nota una oleada generalizada de mitigue, una vez que aparece una acción ejemplificadora de otra compañía, una auditoría interna (o del responsable al encargado), o inclusive el pedido de información para cumplir con DPIA o trámites conexos. Cabría calificar la implementación de SCC y DPA más desde una perspectiva reactiva, que proactiva hoy en día.

[25] WOLFF, J et Al (2021) "*Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020"* – Journal of Information Policy - https://doi.org/10.5325/jinfopoli.11.2021.0063. Recuperado de https://scholarlypublishingcollective.org/psup/information-policy/article/doi/10.5325/jinfopoli.11.2021.0063/291999/Early-GDPR-Penalties-Analysis-of-Implementation. Traducción propia.

Adicionalmente, los costos de consultoría letrada referidos anteriormente, pensando en evitar sanciones difusas y no mesurables, podrían constituirse como un gasto adicional genera una carga económica significativa e imposible de provisionar, más aun entendiendo que se trataría de involucrar recursos (tiempo de un estudio externo especializado, o inclusive un recurso adicional para *headcount* interno que se ocupe de estas revisiones implicando el caudal) para adaptar las políticas a diferentes jurisdicciones con SCC tan variadas.

Un último dato para poder considerar a nivel sancionatorio es el riesgo acarreado por la no implementación de SCC ante paradigmas tan inconmensurables entre sí. Lo antedicho, se evidencia en la posibilidad de tener transferencias tan complejas con cuerpos normativos disímiles, que la violación a los derechos de los titulares no pueda ser debidamente compensada ante una eventual sanción, por la complejidad de coordinación y concentración de información relacionada.

El riesgo en este caso, es configurar inseguridad jurídica para ambas partes: para la empresa, al desconocer a qué nivel de cumplimiento se espera que se ubique (difiriendo en la práctica a las instrucciones del responsable de tratamiento), se desconoce qué nivel de cumplimiento e implementación práctica se refiere (pese a que ciertos recursos se pueden encontrar cubiertos en casuística como por ejemplo las guías de roles entre *controller,* responsable del tratamiento*,* y *processor*, Encargado del tratamiento, del Comité Europeo de Protección de Datos (EDPB, por sus siglas en inglés)), no existe un detalle tan cobertor de todas las contingencias posibles ni jurisprudencia suficientemente uniforme para establecer criterio en todos los casos.

Finalmente, a manos de los titulares de datos personales, el riesgo de inseguridad jurídica se representa ante una violación que involucra múltiples países, teniendo dudas siquiera de dónde poder comenzar un procedimiento de denuncia.

Esbocemos en el acápite posterior qué posibles soluciones se están encontrando en la situación actual, en diferentes jurisdicciones.

vi. Soluciones actuales

Para lograr entender el fenómeno al que se hace referencia, se mencionarán algunos de los principales cuerpos normativos existentes en materia de SCC, y qué soluciones encontró cada jurisdicción para cubrir esta misma situación:

- SCC: se trata de la normativa más desarrollada a la actualizada, sobre la cual se viene debatiendo, generada a la luz del RGPD, rigiendo sobre el EEE. Posee cuatro módulos de tratamiento: responsable a responsable, responsable a encargado, encargado a encargado y finalmente encargado a responsable;
- Reino Unido: mantiene su propio apéndice con un formato adenda oficial también aprobado al efecto;
- CCE: En este caso se incluye la normativa de Argentina, y asimismo la normativa de Serbia, ya que ambas poseen legislaciones establecidas a la luz del RGPD, sin embargo, limitadas a los módulos 1 y 2 de las SCC, sin contemplar encargado a encargado, ni encargado a responsable como escenarios posibles, lo cual dificulta su aplicación fidedigna ante operaciones de procesamiento;
- Turquía y Brasil: Legislaciones relativamente nuevas, permitiendo diferentes variantes a favor de las partes contratantes (SCC, BCRs, *inter/intra company*, etc.).
- Estados Unidos: Habiendo atravesado una tradición de escudos o cláusulas diferentes, generalmente por rebatidos por reclamos incoados por Max Schrems previamente aludidos, al día de hoy poseen el DPF para operaciones comerciales, sólo en los casos donde el encargado específicamente aplique y obtenga la certificación requerida para considerarlo parte del listado de cobertura como se analizó previamente, lo cual lo torna bastante impopular, al tener una tradición de poca durabilidad en las implementaciones de escudos frente al EEE.

Uno de los argumentos esbozados previamente para expresar la complejidad que este multi cuerpo normativo podría traer, tuvo que ver con la potencial longitud y extensión que la implementación de las SCC tendría, y tiene en un contrato comercial. Tal vez, una posible solución podría ser citar las cláusulas contractuales en numerosos ordenamientos vía referencia; es decir, no sumándolas de manera plena, sino citando su aplicabilidad. El lado positivo, sería el acorte efectivo de la implementación de numerosas SCC.

Sin embargo, el nivel de conocimiento requerido podría aún resultar más elevado, debido a la necesidad de identificar las porciones específicas que requieren atención en particular para poder trasladarlas al documento principal. Por ejemplo, dentro de las Cláusulas Contractuales Estándar, se requiere seleccionar ley, gobierno y cortes aplicables en cláusulas 17 y 18, así como tipo de autorización para la inclusión de *Sub-Processors*, subencargado del tratamiento, en su cláusula 9, y aplicabilidad de opcionales en cláusulas 7 y 13; a lo cual, un letrado sin

conocimiento específico no podría ya sea en plexo completo o por referencia, identificar las cláusulas pasibles de adaptación.

Sumado a lo antedicho, la actualización constante a raíz del dinamismo propio de las transferencias podría llevar a tener que abonar capacitación para un recurso interno, o que el estudio jurídico externo traslade el costo de nuevas capacitaciones y certificaciones a medida que las normativas encuentran nuevas aristas para modernizarse. Por otro lado, la viabilidad de las consultas virtuales en este sentido podría ayudar de alguna manera a sopesar los costos, cual destaca Montaño Hurtado[26], al sostener que podrían presentarse como "*una alternativa rentable y conveniente para los clientes. Estos servicios permiten a los clientes obtener asesoramiento legal a través de plataformas en línea, lo que reduce significativamente los costos y el tiempo necesario para reunirse con un abogado en persona"*.

En definitiva, más allá de los esfuerzos por optimizar recursos y reducir costos mediante herramientas digitales, la complejidad técnica y jurídica que conlleva la correcta aplicación de las SCC mantiene vigente la necesidad de una asesoría experta. La interacción entre distintas normativas, las decisiones estratégicas que deben adoptarse en cada cláusula y la constante evolución regulatoria evidencian que la automatización o virtualización del asesoramiento no ayudan a reemplazar necesariamente los costos que demanda la interpretación profesional ni la planificación jurídica integral que exige este tipo de instrumentos.

En este punto se concentra uno de los principales desafíos del análisis. Pese a que la legislación es aplicable sólo por mera referencia en lugar de incorporar las cláusulas totalmente, no se desdibuja la necesidad de tener un cuerpo especializado que asesore en qué cuerpos incorporar, qué tipo de transferencias encajan en cada módulo, qué consecuencias se tienen si no se puede cumplir con ciertos lineamientos, el diseño de las medidas de organización técnica previstas en las SCC, necesitando pensar en el desafío que representa adaptarse a diferentes marcos legales sin perder la esencia y los beneficios de invariabilidad en materia de protección que las SCC proporcionan. Sin más preámbulo, se indagará más en qué desafíos se encuentran en la actualidad a nivel técnico en este espectro.

[26] MONTAÑO HURTADO, J et Al (2023) *"Impacto de la tecnología en la abogacía: cambios en la práctica legal en la era digital"* - - Código Científico Revista de Investigación, 4(E1), 254-269 – Recuperado de http://www.revistacodigocientifico.itslosandes.net/index.php/1/article/view/96/197 - Pp. 262.

vii. Desafíos existentes

Uno de los principales interrogantes que surgen en la práctica consiste en determinar cómo identificar la existencia de una transferencia internacional de datos personales y, en consecuencia, la aplicabilidad de las SCC.

Ya con la propia normativa principal en la materia (GDPR) se representa la problemática en que no existen interpretaciones uniformes sobre cuándo las SCC, y qué módulo deberían ser aplicados, primando discusiones como la aplicabilidad y correspondencia de un Módulo IV (encargado a responsable) donde no existe la posibilidad de declarar subencargados, debatiendo si esa formulación resulta suficiente desde alguna perspectiva, dejando en términos generales la discusión a decisión del responsable y difiriendo a su criterio.

En términos de negocio, el riesgo de convertir al accesorio de las SCC como cobertores de la relación jurídica fundamental en una pieza fundamental, se torna plausible. Lo antedicho, obedece a la complejidad técnica que representa para el negocio tener que recopilar información sobre localización de todo el personal que va a interactuar con ese dato, servidores, los espacios físicos y remotos donde ese dato va a ser accedido, entre otras variables, dependiendo del alcance de los servicios. En términos generales se detecta una tendencia al incumplimiento del requisito por dificultades operativas de cubrir todas las variables, más aún al no existir una sanción concreta como incentivo disuasorio para ponderar la provisión.

Asimismo, el estándar de la industria varía mucho respecto a qué tipo de entidad se analice. El caso más dificultoso de llevar a la práctica puede considerarse en la empresa de tecnología, donde el procesamiento completo comienza y termina a través de procedimientos automatizados sin tener punto de contacto alguno, resulta dificultoso determinar cómo dar cumplimiento al requisito de listar un punto de contacto del subencargado, debido a la naturaleza de la estructura en la que se manejan, donde el punto de contacto podría hasta incluso, ser una Inteligencia Artificial. Lo antedicho, deriva en conflictos operativos e impedimentos administrativos de difícil solución para el negocio involucrado.

A fin de sistematizar los desafíos existentes, es posible agruparlos en ciertos ejes principales. Por un lado, la dificultad de aplicación y obtención de certeza de cumplimiento en la práctica propio del nivel de complejidad que los requisitos teóricos fijados por la autoridad de aplicación poseen. Ello se traduce en la engorrosa configuración que se presenta a nivel roles,

intentando generar un "encastre" de la práctica en la teoría, en tipos jurídicos predeterminados (sin contar los numerosos cuerpos legales aplicables sobre transferencias internacionales de datos personales, casi superpuestos analizados previamente), tornando de casi imposible ejecución la certeza de generación de bases contractuales aplicables a más de un alcance de servicios específico, aún dentro de la misma empresa.

En este sentido, la doctrina empieza a alinearse en torno a la necesidad de comenzar una revisión legislativa más exhaustiva. De Guzmán Plasencia Medina[27] sostiene en este aspecto que "*Aunque en este momento una modificación completa del RGPD podría ser prematura, resulta fundamental que las autoridades de protección de datos sigan vigilando de cerca las nuevas dinámicas y retos que surgen en la gestión de datos personales. La tecnología avanza a un ritmo vertiginoso, creando formas más sofisticadas de recopilar y analizar datos, lo que aumenta la necesidad de mantener y reforzar salvaguardas efectivas que protejan el derecho fundamental a la privacidad".*

En línea con lo antedicho, la inseguridad jurídica toma un rol preponderante, y se traslada no sólo hacia un impacto sobre las partes a nivel interno respecto a la exigibilidad de sus obligaciones, sino que posiciona a los contratantes en un escenario de incertidumbre mayor respecto a potenciales sanciones dependiendo la ley que resulte aplicable en dicha circunstancia.

Finalmente, la falta de alineación de incentivos, así como la opacidad de la propia normativa por las razones esbozadas, genera una reticencia general por parte de los operadores de mercado, a aplicar la normativa en seguimiento exegético de la ley que regule las transferencias en cuestión, prefiriendo ser esquivo al cumplimiento asumiendo la falta de fiscalización, sin ponderar el impacto que tiene sobre sí (limitando el impacto de responsabilidad (a través de un tope en el monto de responsabilidad adquirida) , y sobre los titulares de datos personales.

viii. Implicancias prácticas adicionales

[27] DE GUZMÁN PLASENCIA MEDINA, F. (2025) *"IA y privacidad: Armonización Normativa y Retos Regulatorios en la Unión Europea y España"* – Revista D'Internet Dret I Política – ISSN 1699-8154 – Recuperado de: https://raco.cat/index.php/IDP/article/view/432048/526844

El presente apartado parte de la observación de un dictamen emitido por el EDPB dictada en el mes de octubre 2024, donde se profundiza en la necesidad e importancia de declarar todos los detalles dentro del mapa de datos y Flow de información, principalmente frente a los TIA (*Transfer Impact Assessment*) o DPIA, remitiendo a favor del *controller* (en términos de RGPD) o responsable del tratamiento de los datos personales, facultades para solicitar más información.

Como contracara, el *processor* o Encargado del tratamiento, acaba por encontrarse posicionado en una situación más desventajosa en comparativa. Lo antedicho, en sentido que la opinión referida impone responsabilidades prácticas adicionales por parte del encargado del tratamiento, como el hecho de no culminar su obligación de informar al *controller* sólo en sus propios *sub-processors* o sub-encargados del tratamiento, sino que más aún debe informar un grado adicional en la cadena como los propios *sub-processors* del encargado que él mismo ha designado, alargando un paso más en la necesidad de declarar información al *controller* (entrando más en detalle de este caso en específico más adelante, en el acápite "12.b").

Como problemas en este aspecto, podría entenderse que, ante un marco jurídico general, se puede hacer una analogía al instituto de la "prohibición de regreso" en el derecho penal. Lo antedicho, ya que en dicho instituto no se puede concatenar a cada interviniente sin relación alguna con el hecho pero que haya meramente intervenido de manera operativa, con el resultado final. Un ejemplo, se constituye en el caso donde un taxista que sin mayor interés que la generación de lucro por la prestación del servicio de transporte, lleva a un potencial homicida al domicilio donde va a cometer el delito, sin por ello tener responsabilidad penal alguna sobre el resultado muerte.

Más aún, con el esquema globalizado en el cual la operatoria comercial se encuentra inserta, las transferencias de datos personales a nivel internacional son más comunes de lo pensado. Imagínese que una empresa de pequeño o mediano porte contrata un proveedor local, cuyo servidor de datos utilizado se ubica en un país foráneo, que no se considera adecuado.

Esta situación coloca al *processor* en una posición donde debe demandar información adicional a lo que se consideraba estándar, y no sólo ello, sino que el mismo *processor* debe colocar en lugar mayores salvaguardas para poder contratar proveedores que tengan su operatoria con base global.

Huelga aclarar que esta situación resulta regulada desde lo teórico por el EDPB, sin embargo, la comunidad jurídica que en términos prácticos es quien termina aplicando las previsiones del

RGPD y en este caso las SCC, se encuentra en su mayoría un poco reticente a la aplicación al pie de la letra del contenido de esta opinión, entendiendo la dificultad que su aplicabilidad conlleva.

Desde una perspectiva práctica, estos nuevos requerimientos guardan una relación directa con el objeto central de la presente tesis, referido a la simplificación global de las SCC. Puede afirmarse que, la armonización de las cláusulas contractuales tiene una incidencia directa en esta situación, ya que permite unificar bajo un mismo criterio de aplicación este tipo de vicisitudes que pueden llegar a generar una disputa adicional sobre la aplicación territorial, o no, de dicho tipo de requerimientos, en un contexto de negocios específico.

Lo antedicho, se agrava como se anticipó párrafos arriba, con la interacción tecnológica que amplifica el abanico de transferencias internacionales, no sólo limitándolas a la generación de envíos donde "físicamente" se envíen datos personales, sino también contabilizando los esquemas de trabajo remotos, más acentuados hoy en día con el nomadismo digital, donde la transferencia de datos podría estar realizándose hacia empleados que meramente accedan visualizando una pantalla compartida de su colega que se encuentra ubicado en un país donde el dato personal se encuentre originado.

ix. Avances hasta la actualidad

, A lo largo del presente escrito, se han analizado la existencia de diferentes legislaciones, atomizadas, cada una con la intención de cubrir las propias contingencias que el territorio para el cual fue creada considera relevantes desde un punto de vista político y funcional.

Se demostró que avanzar hacia esquemas regionales de cooperación y reconocimiento mutuo, inspirados en el modelo del RGPD en la Unión Europea, donde se demuestra la posibilidad de poder trabajar de forma armonizada como faro, pero adaptados a los contextos específicos, permitiría reducir costos de cumplimiento, mejorar la seguridad jurídica y fortalecer la competitividad empresarial.

Inclusive sumando tres países que no corresponden con el espacio conjunto de miembros de la Unión Europea en sí (EEE), adicionando a Noruega, Islandia y Liechtenstein a su alcance en términos de aplicación (sin por ello dejar de considerar el principio de extraterritorialidad previsto en el artículo 3 de su texto). Cabe observar aquí ciertas configuraciones ya existentes

en términos de derecho de la integración, como fueran el ASEAN, y su versión "+3"[28] como un antecedente significativo.

Sin embargo, persisten limitaciones derivadas de no poseer un ámbito de institucionalización supranacional ya internalizado como sí ocurre en la Unión Europea, al existir un interés en la armonización de contenido legislativo evitando recaer cíclicamente en las mismas complicaciones que poseemos hoy en día con la legislación atomizada existente.

En Latinoamérica, doctrinariamente ciertos doctrinarios tales como Belli,[29] han indagado en la posibilidad de regionalizar el modelo latinoamericano, tendiendo a fomentar estándares de adecuación generalizados. A saber, rresulta imprescindible acelerar los procesos de actualización legislativa. Se entiende de todos modos, que la cuestión por más viable y delineada que fuere desde un punto de vista teórico legal, encuentra obstáculos político-históricos, pudiendo citar principalmente la falta de acuerdos de integración que congloben a todo el cono sur y las disidencias existentes entre los países que componen la región.

El problema en mantener el esquema atomizado tal como se lo conoce yace en tener que manualmente comparar legislaciones que no parten de bases con fundamentos análogos. Tener particularidades propias de cada región, es decir, algún tipo de porción de los documentos debería tener una parte "personalizable", a saber, una serie de cláusulas aplicables a cada territorio, o removibles como cláusula opcional si las partes determinaran por cierta razón la imposibilidad de cumplimiento, o simplemente desearan removerla por no encontrarse el país bajo el cual esas cláusulas resultan relevantes, o vinculantes, dentro del alcance de los servicios.

Asimismo, la dificultad relativa a la diferencia de profundidad en la tradición en la materia que posea cada país puede presentarse como un punto clave de comparación, en el cual varias legislaciones quedan en un foco de desfasaje, donde sus previsiones resultan muy inferiores a las poseídas en otras legislaciones (el caso actual si a todas se las comparase con el caso del RGPD y las SCC).

Las complicaciones geopolíticas, lingüísticas y hasta culturales, podrían ser un punto de dificultad adicional que imposibilite una implementación tan ambiciosa. Como solución

[28] Adición de China India Corea.

[29] BELLI, L., NOUGRÉRES, A., MENDOZA, J., PALAZZI, P., REMOLINA, N. (2023). Hacia un modelo latinoamericano de adecuación par la transferencia internacional de datos personales. Discussion paper presentado en la Computers, Privacy and Data Protection Conference Latin America (CPDP LatAm) 2023 para recibimiento de comentarios. Versión consolidada en "Protección de datos personales: doctrina y jurisprudencia. CETYS, CDYT, 2023, Buenos Aires. Recuperado en fecha 11/4/2025 de https://cpdp.lat/wp-content/uploads/2023/07/doc-discusion-cpdplatam23-2.3.pdf pp.1 y ss.

intermedia, tal vez pensar en acuerdos bilaterales y multilaterales sea una chance potencialmente creable.

En vista de este panorama, aparentaría que la fragmentación normativa actual en protección de datos plantea desafíos importantes. Si bien el RGPD aparentaría demostrar que la armonización es posible, globalmente persisten obstáculos políticos e históricos que dificultan un modelo común. La solución intermedia, podría ofrecer un camino viable hacia una mayor coherencia normativa sin perder de vista las particularidades locales, por lo cual se analizarán posibles propuestas.

x. Posibles propuestas

Llevado a la práctica, debemos cuestionarnos qué posibles soluciones se podrían aplicar, en el contexto actual. Y es verdad, la cantidad de alternativas entre las cuales seleccionar hoy, podría aparentar ser relativamente baja. Sin embargo, se parte de la base de lo existente, para comenzar a profundizar a medida que se avance el análisis.

Indiscutiblemente las SCC conexas al RGPD, e incluso la propuesta del *Information Commissioner's* Office del IDTA (Reino Unido), poseen una estructura que podría verse como punto base para el análisis que en marras atañe. En ambos casos, estamos ante cláusulas contractuales que, en términos politológicos, operan como una suerte de "boleta única" con una cierta cantidad de opciones o cláusulas opcionales, generalmente traducidas en una cantidad establecida de casilleros a llenar.

Podrían analizarse ventajas y desventajas de esta perspectiva, para entender si es una posible propuesta si pensamos en armonizar la normativa, idealmente, a nivel global. Como ventaja, cabe pensar en un único cuerpo, de consulta obligatoria siempre que existiese una transferencia, redactado de manera condicional de modo que sus cláusulas sólo aplican si existe una transferencia entre los países que tiene como objetivo cubrir.

Adicionalmente, podría estandarizarse bajo distintos grupos de secciones, inclusive armonizando entre ciertos países, bajo los cuales se considere más o menos relevante la aplicabilidad de cierto *safeguard* o salvaguarda. Lo antedicho, facilitaría En que principalmente, en vez de contar con numerosos cuerpos dispersos a ser fusionados en un mismo documento, se contaría con un documento único, del cual se puedan remover

determinadas secciones si las partes las entendiesen como “no aplicables” (e inclusive en la práctica, si todas se dejasen, no conflictuarían entre sí).

Más aún, respecto a los roles, la dificultad de poseer roles estancos y rígidos complica la cobertura en casos donde un *processor* quiere contratar con un *controller*, pero no necesariamente es “su” *controller* o responsable con respecto a él. Un ejemplo, se da cuando un proveedor de datos, que tenga su propio *pool* de manera previa, es contratado por un *processor* actuando en nombre de otro *controller*. Inclusive, la forma en que están redactados los *templates* de las SCC y su invariabilidad, genera que la existencia del módulo IV, encargado (exportador) a responsable (importador), no posea un acápite de subencargados, lo cual inclusive complica su aplicabilidad fidedigna con la realidad empírica.

Ahora bien, como desventaja, podría encontrarse una disimilitud de lenguaje, longitudes de cada uno de los apéndices de cláusulas, qué país sería el que establece las cláusulas, e inclusive, si no se armoniza correctamente, es posible hallar superposiciones y choques internos de la propia letra de la ley (y sus autoridades de aplicación). Básicamente, se podrían alegar aquí las contras propias de todos los sistemas concentrados.

Más allá de la manera en la cual ejecutar la armonización, se encuentran otras implicancias dignas de ser mencionadas. En primer lugar, los profesionales legales necesitarían menos formación especializada sobre normativas locales, reduciendo costos de capacitación. Menos certificaciones, y mayor conocimiento y actualización propia sobre la vida y las implicancias del documento. Facilitaría el diálogo entre profesionales de distintas partes del mundo, todos partiendo del mismo bagaje teórico para luego dar lugar a sus interpretaciones locales, propias del área de privacidad.

A nivel autoridad de aplicación, podría pensarse en un organismo *ad hoc*, lo cual no es imposible de ser imaginado, con la existencia de organismos globales como es el caso de la Organización de las Naciones Unidas (ONU). Sin embargo, por la diferencia en criterios de sensibilidad, por ejemplo, incluso poseyendo criminalizadas ciertas categorías en determinados países del mundo, sería uno de los puntos más álgidos a considerar, sobre cómo estructurar cierta rotación en la cual los dictámenes y opiniones consultivas de interpretación sean emitidos por cuerpos colegiados que representen diversos intereses, idealmente, rotativos.

El documento único tiene sus ventajas en la consolidación, sin embargo, el costo y demanda de actualización constante de un documento cuyo contenido representa tal nivel de dinamismo

y *momentum* con la realidad tecnológica actual, podría representar valores no previstos al día de la fecha en materia de privacidad de datos.

Empresarialmente, reduciría la necesidad de tener tanta documentación variada, y sería un único documento al cual acudir para este tipo de situaciones. Sin embargo, el dinamismo propio de la naturaleza de las transferencias internacionales en un contexto tecnológico globalizado lleva a la doctrina a pensar que este tipo de soluciones no son necesariamente perpetuas (ni duraderas).

Interpretando a autores como Rzayeva[30], se comienza a sostener, que los expertos jurídicos especializados en leyes internacionales de protección de datos deben realizar una revisión periódica del panorama legal en los países receptores, enfocándose en los cambios en las leyes de protección de datos, las prácticas de las autoridades de control y las decisiones judiciales que puedan afectar el nivel de adecuación en materia de protección de datos.

Lo antedicho, dejando ver que no sólo depende de la necesidad de actualización por parte de los profesionales del área, adaptándose a la normativa dictada dinámicamente, sino más aún, pudiendo estar sujeto a decisiones jurisdiccionales que pueden modificar el panorama, disparando nuevas necesidades de actualización en materia de protección de datos, por parte de los actores intervinientes.

Finalmente, y una preocupación que podría llegar a analizarse, tendría como eje el potencial futuro de los profesionales, entendiendo que un documento único, personalizable, con mandas claras, podría hasta ser *customizado* con inteligencia artificial. Sin embargo, este tipo de argumento resultaría simplista, ya que, de otro modo al día de la fecha, los documentos oficiales de las SCC y cláusulas modelo también podrían representar este riesgo, y en la práctica son de los tópicos más candentes de discusión a la hora de debatir su aplicabilidad.

xi. Análisis de regímenes de unificación.

Pese a los numerosos intentos frustrados de realizar una unificación en este sentido, y anticipando a las conclusiones que efectivamente se comenzarán a dirimir en el párrafo

[30] RZAYEVA, J. (2024) - "*Standard Contractual Clauses as a GDPR safeguard: implementation and challenges"* Vilnius University Faculty of Law - Department of Private Law – Recuperado de https://epublications.vu.lt/object/elaba:191367268/ - Pp. 38 – Traducción propia.

subsiguiente, la pregunta que queda realizarse es, ante el panorama existente en la materia: ¿Bajo qué régimen es conveniente unificar?

La respuesta es bastante clara. A la fecha, las normativas en materia de privacidad de datos han ido replicándose y multiplicándose en diversos niveles: si consideramos el caso del RGPD nos referimos a una normativa regional, el caso de PIPEDA (*Personal Information Protection and Electronic Documents Act*) una normativa Nacional atinente a Canadá que aplica al sector privado para organizaciones que coleccionan, usan o revelan Datos Personales[31], y finalmente si hablamos de CPRA (*California Privacy Rights Act)* modificatoria de CCPA *(California Consumer Privacy Act),* estamos refiriéndonos a una normativa local o estadual que apunta a aplicar principalmente sobre el estado de California en los Estados Unidos. Sin embargo, la cantidad de leyes afloradas recientemente en términos cuantitativos no logra aplacar el "faro" que es considerado el RGPD, no sólo por ser la normativa más relevante a la fecha, sino asimismo por encontrarnos con numerosas legislaciones locales alineadas con los principios que el RGPD contiene, sin ir más lejos, analizando el caso de Argentina.

Más aún, el estándar al cual los países que actualmente se consideran adecuados han intentado consistentemente arribar, se basa en los estándares fijados por el RGPD, por lo cual esta armonización se presentaría como la más amena en términos de costumbre de la comunidad legal internacional.

Desde otra perspectiva, la posible subsunción a otro tipo de legislaciones, como podría por ejemplo ser PIPA (*Personal Information Protection Act*) en Corea del Sur, estaría colocando en riesgo otra serie de factores en posible conflicto con principios internacionales. A saber, la imposición de penas como el posible envío a prisión en ciertos supuestos del régimen de protección de datos, podría llegar a entrar en conflicto con los diversos códigos penales existentes a lo largo del mundo, lo cual complicaría la adhesión ante posibles principios de regresividad en materia de derechos adquiridos.

Asimismo, unificar bajo legislaciones que asimilen al RGPD pero que aún no se encuentren a su nivel de avance, podría implicar un retroceso en los derechos y operatorias ya consolidadas a nivel global. Un ejemplo de ello, podría ser la potencial unificación bajo el régimen serbio o argentino, donde los esquemas de transferencia contemplados en los "Módulos" o "Anexos"

[31] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. (2020). Privacy Guide for Businesses: PIPEDA (Cat. No. IP54-94/2019E). Gobierno de Canadá. Recuperado de https://www.priv.gc.ca/media/2038/guide_org_e.pdf

de sus cláusulas contractuales estándar, sólo contemplan la relación responsable del tratamiento a responsable del tratamiento (*Controller to Controller*), o responsable del tratamiento a encargado del tratamiento (*Controller to Processor*), dejando por fuera los vínculos entre encargados del tratamiento (*Processor to Processor*). inclusive el caso en que un encargado del tratamiento exporta datos personales a un país no adecuado (*Processor to Controller*).

En consecuencia, aun cuando la unificación normativa bajo un marco común aparece como un objetivo deseable en términos teóricos, su implementación práctica plantea obstáculos significativos vinculados tanto a la heterogeneidad regulatoria existente como a las divergencias en el grado de desarrollo institucional de cada país. Estas tensiones evidencian que la armonización formal de los textos legales no necesariamente garantiza una aplicación uniforme ni efectiva en la práctica, dando lugar a una brecha entre el diseño normativo y su operatividad real. Es precisamente en ese punto donde cobran relevancia los desafíos prácticos que emergen al momento de trasladar las previsiones jurídicas a esquemas de cumplimiento concretos.

xii. Desafíos de aplicación práctica

Se ha intentado a lo largo del presente documento cubrir las vicisitudes que la aplicación de normativa regente en materia privacidad de datos posee ante la efectiva realización de transferencias internacionales de datos personales, no sólo a países adecuados sino más aún a países cuya transferencia requiere salvaguardas legales adicionales, como fueran las SCC, cláusulas modelo o instrumentos conexos.

Ahora bien, existen diferentes desafíos en la aplicación práctica de las normativas previamente aludidas, ya que la complejidad de la transferencia globalizada de datos personales dificulta la cristalización de las relaciones prácticas en acuerdos escritos entre las partes.

Contingencias podrían ubicarse de manera múltiple, y más aún, variando la cadencia de localización de estas dependiendo la industria bajo la cual nos encontremos analizando la transferencia, los países involucrados, y las categorías de datos que estén siendo procesados.

Sin embargo, en línea con las dificultades que venían analizándose y trabajándose a lo largo de la presente tesis, se concentrará el análisis en dos ejes que dificultan la aplicación práctica a rajatabla de los lineamientos establecidos por las autoridades de aplicación.

a. Rigidez normativa como obstáculo de traducción fidedigna del procesamiento.

En primer lugar, la dificultad de ubicar ciertas relaciones de procesamiento dentro de los compartimientos estancos que las cláusulas contractuales proponen.

Existiendo situaciones donde las partes contratantes no necesariamente se componen por un responsable de tratamiento y su encargado, sino que se trata de un responsable del tratamiento que va a dar acceso a, retomando un ejemplo previo, su propia base de datos a favor de una parte que opera como encargada del tratamiento a favor de un tercero responsable del tratamiento, acaba por configurar un esquema aún no zanjado a nivel normativo en lo que respecta a cláusulas de transferencia internacional de datos.

Es interesante destacar la imposibilidad práctica por parte de la parte contratante de lograr capturar de manera fidedigna la relación con el tercero (en este caso hipotético proveedor de base de datos), al no poseer un módulo en el cual encuadrar esa transferencia.

Lo más cercano, podría llegar a ser un Módulo 1 de las SCC (*Controller to Controller*), que asegura *compliance* con la regulación[32], a ser suscripto entre el tercero proveedor de datos desde su propia base de datos, junto con el responsable de tratamiento que efectivamente manda a realizar el trabajo de procesamiento al encargado. La dificultad práctica en este caso se revela en diferentes aristas.

La falta de flexibilidad en los roles previstos puede llevar a situaciones en donde no quede claro de qué manera instrumentar un contrato que permita cubrir la vinculación que las partes por primacía de la realidad poseen, contingencia que acentúa su impacto en el caso donde la operatoria en materia de transferencia internacional de datos personales no se encarna en un flujo tan claro que habilite colocarlo en agenda, como sí ocurre en países parte del espacio económica europeo.

Si se ahondara en la razón, podría ubicarse como la deficiencia de procedimientos sancionatorios por parte de las agencias y autoridades de aplicación podrán esbozarse como la razón principal. No resulta una cuestión primordial mitigar un riesgo que no se traduce en un potencial perjuicio económico.

[32] Official Journal of the European Union. COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

Puede tomarse el caso local como ejemplo. Más allá de considerar a la normativa argentina con un nivel adecuado de protección de datos, la existencia de una agencia bicéfala con intereses diversificados y procedimientos sancionatorios cuya aplicación práctica no alcanza a tener una magnitud que disuada a los responsables y encargados del tratamiento de operar y llevar a cabo sus flujos de datos sin cubrir específicamente la relación de procesamiento que constituyen, es difícil pensar que se invertirán recursos suficientes (tiempo de dilación en la firma del contrato, contratación de cuerpo letrado especializado) para poder llegar a una situación donde una consulta local a la autoridad de aplicación motive a la creación de nuevas relaciones, novedosas, contempladas a nivel legal. Se entiende que el escenario antedicho, aunque idílico, resulta de aplicación dificultosa, sino imposible.

Los intereses económicos sólo se alinearán con el espíritu de protección legal si los procedimientos sancionatorios que deberían tener como objeto la protección de datos personales de los sujetos titulares de los mismos, operan con un impacto suficiente como para merecer la atención de quien subyacentemente tiene una relación jurídica fundamental primaria en vista: la persecución y ejecución del negocio en el cual efectivamente están procesando los datos personales aludidos.

Este desfasaje, aunque existente en el área de privacidad de datos, no es exclusivo del fuero. En áreas como derecho administrativo general, doctrinarios como Vaca[33] sostienen que se "*progresa en la regulación del uso de herramientas tecnológicas y la salvaguarda de la información personal, pero aún se topa con lagunas legales y técnicas que obstaculizan una aplicación eficaz y homogénea en el sistema judicial"*, refiriéndose al sistema judicial ecuatoriano específicamente. Dicho esto, la relevancia del tópico resulta trasladable a áreas que inclusive exceden la órbita del derecho en materia de privacidad de datos personales.

Se confirma de todos modos con lo antedicho, que la opacidad propia del lenguaje que manejamos en el área jurídica, y mucho más en este nivel de especialidad en la materia, opera como un limitante adicional, pensando que quien debe tener las herramientas para levantar este tipo de riesgos inicialmente, es el área de negocios. Sea que estemos dentro de una estructura organizacional donde meramente se requiera un levantamiento de ticket, o en el ámbito independiente donde haya que realizar una efectiva llamada a un abogado especialista,

[33] VACA-ALDAS et Al "Protección de datos personales en la gestión de justicia: análisis del marco normativo ecuatoriano frente a los estándares internacionales" - 593 Digital Publisher CEIT, ISSN-e 2588-0705, Vol. 10, Nº. 3, 2025 - Universidad Bolivariana del Ecuador - Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=10287447 Pp. 1067.

necesitamos proveer al área de negocios, a quienes poseen su *core business* en la ejecución de nuevas interacciones que requieren la atención jurídica ulterior, de instrumentos en lenguaje llano que les permitan identificar la existencia de una relación jurídica de procesamiento de datos personales, que amerite una cobertura contractual específica.

Más aún, el incentivo económico de encontrarse mitigando un riesgo traducible en dinero, es una cuestión fundamental para entender la relevancia que la actualización normativa tiene en este sentido.

b. Ausencia de aprovechamiento y aplicación análoga de experiencias en otras áreas.

Los rigorismos formales pueden tener como contracara la imposibilidad de aplicación de los mismos en la práctica, o aún más, configurar un escenario donde llevar a cabo los procedimientos establecidos legalmente, resulte tan costoso y difícil, que en vez de fomentar niveles de cumplimiento razonable por quienes, en este caso, se encuentren procesando datos personales, acabe por configurar un escenario donde ponderando costo y beneficio, sea más beneficioso para las partes saltear la aplicación de normativa legal en materia de privacidad de datos (más aún sin incentivos económicos globalmente uniformes firmes para aplicarlas), y acabe porg

Muy concretamente se tomará un ejemplo al que ya se hizo mención previamente, contando cómo la opinión 22/2024 (Dictamen 22/2024, citado en Bibliografía obligatoria, desde aquí el "Dictamen") viola el aprendizaje y fundamento legal de la prohibición de regreso, propia de materia penal.

En primer lugar, se toma la definición de Jakobs[34] al sostener que la prohibición de regreso puede entenderse como "*La prohibición de recurrir, en el marco de la imputación, a personas que si bien física y psíquicamente podrían haber evitado el curso lesivo –hubiese bastado tener la voluntad de hacerlo–, a pesar de la no evitación no han quebrantado su rol de ciudadanos que se comportan legalmente".* En este sentido, se toman elementos como la posibilidad de evitar el curso lesivo, y la razonabilidad que la doctrina achaca a ese *iter*, así como el "rol" de ciudadanos del que se habla, entendiendo que en este caso están refiriéndose a personas físicas dentro del área penal.

[34] GUTARRA, A. (2019). La teoría de la prohibición de regreso. Revista pensamiento penal. Recuperado en fecha 8/3/2025 de: https://www.pensamientopenal.com.ar/doctrina/47313-teoria-prohibicion-regreso

El Dictamen referido, alude a la responsabilidad de los encargados y subencargados del tratamiento, así como también refiere a la relación contractual que debe unirlos a lo largo del procesamiento de datos. Una de las cuestiones centrales del análisis, se basa en la pregunta práctica sobre qué relaciones contractuales quedan a cargo del responsable del tratamiento; es decir, si su obligación se agota en colocar un contrato con el encargado directo del tratamiento y obligarlo en los términos de los artículos 28 a 30 del RGPD a colocar contratos análogos y equivalentes con los subencargados que el mismo designe, o si por el contrario, el responsable del tratamiento está legalmente obligado a tener control sobre todos los contratos con subencargados y encargados independientemente del eslabón de la cadena de procesamiento donde ellos se encuentren ubicados, salteando todo tipo de intermediario.

Desde la práctica, la respuesta resultaba bastante inducible. Sin embargo, en el considerando 21, punto 2.1.1 del Dictamen, se señaló que "*El responsable del tratamiento debe identificar a todos los subencargados del encargado, sus subencargados, etc. a lo largo de toda la cadena de tratamiento, o solo identificar la primera línea de subencargados contratados por el encargado, el CEPD recuerda, en primer lugar, que «A pesar de que la cadena puede ser bastante larga, el responsable del tratamiento conserva su papel central en la determinación de los fines y medios del tratamiento"*.

Así, profundizando en el considerando 31 que "*Aunque esto no es explícito en estas disposiciones, el Comité considera que, a efectos del artículo 28, apartado 1, y del artículo 28, apartado 2, del RGPD, los responsables del tratamiento deben tener la información sobre la identidad de todos los encargados del tratamiento, subencargados, etc., fácilmente disponible en27 todo momento para que puedan cumplir mejor sus obligaciones en virtud de las disposiciones mencionadas anteriormente. Dicha disponibilidad también es necesaria para que los responsables del tratamiento puedan recopilar y evaluar toda la información necesaria para cumplir los requisitos establecidos en el RGPD, en particular para que puedan responder a las solicitudes de acceso con arreglo al artículo 15 del RGPD sin demoras indebidas y reaccionar rápidamente ante las violaciones de la seguridad de los datos que se produzcan a lo largo de la cadena de tratamiento. Esto se aplicaría independientemente del riesgo asociado a la actividad de tratamiento"*.

Desde una perspectiva teórica, lo antedicho hace sentido: quien contrata, es responsable por sus dependientes, principio del derecho civil debidamente contemplado. Ahora bien, a nivel práctica, entender que los párrafos previamente citados revelan la necesidad del responsable

del tratamiento de requerir al encargado que liste no sólo a sus subencargados, sino a los subencargados de segundo nivel en la cadena, e incluyendo la referencia "etc." o etcétera, no fija límite alguno sobre cuándo se finalizaría esa cadena de listado y responsabilidad.

En este sentido, es donde la analogía con el instituto de la prohibición de regreso, sería un activo infalible: con el criterio de responsabilizar al responsable del tratamiento del total de la cadena, sin limitación ni parámetro de razonabilidad alguno, la dificultad que surge evidente es que al transpolar ese criterio en la prohibición de regreso, sería el equivalente a responsabilizar como partícipe necesario al taxista que lleva al homicida a cometer el delito, sólo por el hecho de haber participado en la cadena.

En el área penal, se trata de una discusión zanjada: nadie culpabilizaría a quien cargó nafta en el vehículo que transportó al contrabandista sólo por el hecho de participar en la cadena. Sin embargo, en materia de protección de datos personales, el Dictamen aparentaría colocar a la situación en un gris, ¿por qué no resulta válido el contrato entre parte responsable y primera línea de encargado, donde el encargado por el RGPD ya está asumiendo responsabilidad total por los subencargados, así como también por hacer un *flow-down* de las mismas obligaciones, adquiriendo de esa forma la obligación de imponer sobre sus subencargados la necesidad de listar a los subencargados que ellos mismos sumen al procesamiento? Por falta de casuística a la fecha, posiblemente.

Más aún, en una situación práctica de aplicabilidad: una empresa de responsable del tratamiento, ubicada en el EEE, contrata una empresa global como encargada del tratamiento. Coloca SCC apropiadas con la empresa, para transferir datos donde la misma presta tareas: Estados Unidos y Serbia. Sin embargo, al tener la responsabilidad de listar a todos sus subencargados sin límite de nivel, la compañía responsable debe asegurarse de obtener el listado de todas las líneas de subencargados, inclusive de los proveídos por empresas de índole *software as a service.*

Esta opinión es sólo un ejemplo. La atomización, abre el juego a la posibilidad en que cada autoridad de protección de datos emita sus propias interpretaciones, y con ellas, cada abogado, funcionario o inclusive empresario, de lugar a su propia lectura de estas por sí solo. El resultado, acaba siendo la segregación de la interpretación legislativa, en donde los encargados y responsables del tratamiento ubicados en ciertas zonas donde territorialmente se haya dictado una otra opinión de esta índole, posean una interpretación más o menos radicalizada, que dilate las negociaciones a niveles impensados, con requisitos que acaban por tergiversar el fin último

de la ley, a la luz de solventar requisitos excesivamente rigurosos y de aplicación imposible en la práctica.

En este sentido, la atomización continúa poniendo más en jaque el fin último del bien jurídico tutelado, que acaba por ser la protección de los titulares de datos personales procesados para prestar ciertos servicios. Sin embargo, como vinimos expresando previamente, aunque los intentos de regionalización a nivel teórico aparecen incipientemente esquematizados, es difícil imaginar un mundo con normativa de privacidad de datos uniformizada, si la interpretación de las autoridades de aplicación complica cada vez más la posibilidad de cumplir con las mismas en la práctica, y la recomendación legal termina resultando programática, por la excesiva onerosidad de su implementación, acompañado de un potencial riesgo difuso si se omite seguir los lineamientos bajo la literalidad que la ley requiere.

xiii. ¿Regionalización o continuidad?

En este punto, es pertinente cuestionar si el camino correcto es la regionalización o la continuidad. Desde una perspectiva jurídica, la respuesta no puede ser absoluta, sino que depende del contexto normativo y político vigente. La regionalización, entendida como mecanismo para facilitar el análisis, la operatoria de negocios, y abaratar costos de revisión e implementación, se presenta como una estrategia indispensable.

Este punto de partida evidencia una necesidad concreta: si bien el ideal de armonización global en materia de protección de datos personales continúa siendo una meta idealista, la realidad normativa y política demuestra una dificultad evidente para llegar a ella en lo inmediato. Por ello, la regionalización, o inclusive la agrupación en ciertos países, aparece como una alternativa estratégica viable y eficiente.

La posibilidad de avanzar hacia sistemas regionales de protección de datos permite poner en agenda ciertas realidades jurídicas, económicas y sociales compartidas por determinados grupos de países, así como también establece un marco operativo intermedio entre la total fragmentación y la homogeneidad que no resulta lograble en la actualidad.

No por ello se sostiene que la regionalización representaría una “fractura” total al sistema normativo global vigente, por el contrario, se constituiría como un paso ordenado hacia la convergencia. A saber, para que esta regionalización resulte funcional, es fundamental

armonizar la operatoria y los principios que rigen a los diferentes países que suscriban, para evitar se dicten leyes completamente programáticas.

Si se pensara en la continuidad absoluta del sistema, sosteniendo normativas preexistentes sin adaptar a nuevas realidades, estaríamos observando, tal como existe hoy en día, una sobrecarga normativa que desincentiva el cumplimiento real en términos del trabajo cotidiano. Dicho ello, la aparente dicotomía existente entre regionalización o continuidad debe repensarse no como una opción binaria y excluyente, sino como un proceso de convergencia estratégica.

Si se piensa en ejemplos concretos, sin ir más lejos, la reciente emisión por parte del *Department of Justice* (DOJ) de los Estados Unidos, con el reglamento final derivado de la *Executive Order* 14117[35], buscó inicialmente restringir el acceso de países considerados "de preocupación" a datos personales sensibles y gubernamentales de ciudadanos estadounidenses. Sin embargo, ésta refleja un nuevo intento de proteccionismo digital con fundamentos en la seguridad nacional, el cual, ante las primeras aplicaciones prácticas, termina teniendo un efecto contrario al buscado inicialmente.

Lo antedicho, ya que este tipo de medidas, aunque legítimas desde la perspectiva soberana, resultan contraproducentes en la práctica global, pues terminan por aislar a los propios sujetos de datos estadounidenses del flujo internacional de información, generando fricciones con los mecanismos de cooperación y transferencia reconocidos por otras jurisdicciones.

La mera idea de prohibir en una etapa globalizada, en un contexto económico y tecnológico crecientemente interdependiente, la transferencia de datos entre ciertos países, requiriendo inclusive una limitación a nivel societario (convirtiendo en un país prohibido inclusive a las empresas que tuviesen parte de su paquete de control localizado en uno de ciertos países como en este caso Rusia, China, Cuba, Venezuela), acaba por operar como un arma de doble filo, donde económicamente pueden aislarse a los sujetos titulares de datos personales del país que incoa este tipo de normativas, en este caso, Estados Unidos.

Continúa sosteniéndose que la fragmentación normativa y las restricciones unilaterales no fortalecen la protección de los titulares, sino que incrementan la asimetría y el riesgo jurídico en las operaciones transnacionales. La necesidad de generar vínculos jurídicos más fluidos y

[35] Análisis tomado de "BRANSEN, K. (2025) "DOJ Finalizes Rule Prohibiting and Restricting Foreign Transfer of Personal Sensitive Data" – EDUCAUSE REVIEW – Online – ProQuest - Recuperado de: https://www.proquest.com/openview/b70dd3e9a535e85b42ac6dcb61f5c29a/1?pq-origsite=gscholar&cbl=7213897

compatibles entre sistemas es hoy más urgente que nunca: el mundo digital no reconoce fronteras, y las respuestas regulatorias basadas en la desconexión sólo profundizan la brecha que la regionalización o la cooperación internacional buscan precisamente superar.

Regionalizar para simplificar, como primer paso transitorio. Y nuevamente, se traen los principios generales del derecho aquí. Al cuestionarse si es ideal el cupo femenino en ciertas posiciones, la respuesta sería que, si bien no constituye una solución definitiva, representa una herramienta transitoria válida para iniciar un proceso de cambio estructural. Continuar para consolidar los aprendizajes existentes, y finalmente, tender a avanzar hacia modelos de referencia flexibles, con opción múltiple, accesibles, que contemplen el dinamismo del ecosistema digital y respeten el espíritu protector de la normativa sin convertirse en un obstáculo inviable para el desarrollo económico y tecnológico que el mundo globalizado en el que habitamos nos propone actualmente.

VI- CONCLUSIONES

En síntesis, el análisis desarrollado a lo largo del presente trabajo permite confirmar la hipótesis planteada: la armonización global en materia de protección de datos personales resulta actualmente inviable, mientras que la regionalización aparece como una alternativa estratégica viable y necesaria. El conflicto normativo actual en término de transferencias de datos personales a nivel internacional podría ubicarse como la existencia de una tensión entre dos paradigmas opuestos, pero, hasta la actualidad, necesarios. Por un lado, es evidente la urgencia de armonizar estándares, para evitar que la protección de datos personales se transforme en un obstáculo insalvable para los negocios transnacionales, operando como un análisis de descarte, tal cual acaba convirtiéndose en la práctica. En la esquina contraria, la necesidad de mantener cierta flexibilidad y adaptación normativa pese a idear ambiciosamente un paradigma global, respetando y valorando las realidades locales, evitando una homogeneización absurda y falta de crítica que omita variables fundamentales, tornando tal magnitud de esfuerzo, programático por no cumplir su función inicialmente pensada.

En línea con la hipótesis planteada, este trabajo ha partido de reconocer que la armonización global resulta hoy jurídicamente inviable, pero que la regionalización, como proceso

intermedio y adaptable, aparece como una alternativa posible y necesaria para reducir la fragmentación normativa y fortalecer la seguridad jurídica.

Pensar en la viabilidad de una armonización normativa total a nivel global hoy, es mucho más que una meta jurídica, pudiendo esbozarla como un desafío geopolítico y cultural. Al efecto, pensar un poco más a la regionalización, no tanto como una renuncia al ideal de convergencia, sino como un modelo intermedio y necesario con impacto directo en la operativa empresarial global. Una agrupación normativa funcional, que simplifique y facilite la licitud de las transferencias internacionales de datos personales, reduciendo costos de cumplimiento y pensando en comenzar un diálogo que promueva una unificación de criterio entre autoridades, empresas y profesionales que suscriban, sin caer en abstracciones teóricas inaplicables como sería la imposición de un cuerpo existente sin posibilidad de *customización*.

Esta regionalización, como muestran los casos de la Unión Europea y sus Cláusulas Contractuales Estándar (SCC), puede funcionar como modelo base para el desarrollo de marcos regionales flexibles. Su estudio permite identificar variables comunes y proponer lineamientos que faciliten el cumplimiento normativo y la cooperación entre bloques, cumpliendo así los objetivos específicos de identificar marcos comparables y promover coherencia regulatoria.

A nivel práctico, esta estrategia permite pensar en una matriz común de interpretación y evaluación del riesgo normativo, que evite soluciones *ad hoc* excesivamente onerosas, fomentando una cultura de cumplimiento realista y eficiente. Las SCC, por su estructura, podrían actuar como modelos base para desarrollar instrumentos flexibles, adaptables por región, con cajas a chequear y opciones removibles, que permitan el diálogo entre normativas sin exigir una fusión impracticable.

A nivel local, es fundamental colocar la temática de protección de datos en agenda. Existen anteproyectos de actualización a la ley de protección de datos personales local, sin haberse traducido en una efectiva actualización que comience por dar respuesta a las nuevas conformaciones fácticas que las transferencias internacionales de datos personales presentan, ni siquiera adaptándose a los esquemas ya existentes, como los delineados por las SCC del RGPD (Módulos III y IV). Cierto es que en junio 2025 se presentó un proyecto[36] intentando actualizar puntos clave como el interés legítimo, prohibición de cesión masiva de bases de

[36] Texto completo de PROYECTO DE LEY - LEY DE PROTECCIÓN DE DATOS PERSONALES disponible en fecha 3/7/2025 en: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2025/PDF2025/TP2025/1948-D-2025.pdf

datos entre entidades del sector público, cuestiones que acercan a la portabilidad como el derecho del titular de datos acceder a información en lenguaje de su elección, así como la idea del "metadato" o dato inferido, para evitar restricciones exegéticas que perjudiquen derechos bajo meros rigorismos formales. Sin embargo, no es la primera vez que la comunidad jurídica especialista intenta actualizar los términos vigentes, y asimismo no resultaría sorprendente una posible pérdida de estado parlamentario por no tratarse de un proyecto de alto impacto para la agenda jurídico-legislativa, subestimando el impacto y potencial perjuicio que puede acarrear a nivel personal, y a nivel esquemático global (impedimento de gestión de negocios, obstáculos de implementación y conexión con países extranjeros), una potencial pérdida de reconocimiento "adecuado" por parte de la autoridad europea, perjudicando empresarios locales al requerir material documental y análisis adicional en caso de pasar a ser un país no adecuado, si dejáramos desfasar aún más nuestros estándares.

Hay que mencionar que esta situación choca de frente con las recomendaciones técnicas emitidas por la AAIP (Agencia de Acceso a la Información Pública), que desde hace tiempo intenta impulsar reformas concretas para adecuar la legislación a los estándares internacionales en protección de datos personales. En este sentido, el análisis nacional demuestra la necesidad de avanzar hacia una adecuación progresiva de la normativa argentina a los estándares internacionales, en coherencia con la hipótesis de que la convergencia regional constituye un paso previo indispensable hacia cualquier intento de armonización global. Tema en continua evolución normativa al momento de cierre de esta investigación, del cual se anhela tener mayores novedades a la brevedad, dada la sensibilidad del tópico.

Reformulando entonces, puede sostenerse que el estudio permitió comprobar que ninguna de las posturas extremas, ni la armonización total ni la independencia normativa absoluta, resulta sostenible. Por ello, se propone un modelo híbrido que combine una regionalización operativa con un horizonte de convergencia global a largo plazo, aunque no por ello perpetúe una continuidad durante mucho más tiempo. Ello así, ya que la rigidez del modelo vigente conflictúa dos paradigmas diferentes. Por un lado, un paradigma de necesidad de armonización legislativa global previamente aludido, al entender que la rigidez de los roles establecidos en cada una de las normativas, así como la avanzada a nivel criterio por parte de las autoridades de aplicación, complican cada vez más la aplicación por parte de cada empresa al momento de llevar a cabo un negocio donde exista una transferencia de datos personales fuera de los límites nacionales. Ello, al no encontrarse claro en qué momento se puede considerar que una empresa se encuentra en cumplimiento, si se considera la falta de análisis práctico de la normativa que

requiere listar infinitamente la cadena de encargados y subencargados, en un mundo globalizado donde cada lista sólo en un vínculo entre partes, puede contener según el tipo de servicio más de 20, 30 o 50 subencargados diferentes, ubicados a lo largo y ancho del planisferio, con normativas que requieren cada vez más detalle, de imposible obtención, para quienes acaban por encontrar el cumplimiento normativo sólo como un obstáculo económico para poder llevar a cabo el *core business* por el cual desean contratar. Por otro lado, la política del *one size fits all*, tampoco debe caer en la trampa del simplismo absurdo, dejando de lado una cantidad de variables fundamentales para enmarcar las diferentes vicisitudes que normativamente aquejan a cada país o región, permitiendo cierto nivel de personalización del contenido.

Por su parte, pese a que la regionalización conlleva cierto grado de concentración de poder en los órganos encargados de su aplicación como se mencionó en los acápites iniciales, esta característica no debe entenderse como una desventaja insalvable en este caso particular. Por el contrario, en la práctica, la regionalización se erige como una solución viable y tangible frente a la fragmentación normativa actual, al permitir una coordinación más eficiente, una interpretación más uniforme y una reducción significativa de los costos de cumplimiento, sin desconocer las particularidades locales que cada jurisdicción aporta al esquema global.

En términos prácticos, los próximos pasos deben orientarse a la cooperación entre regiones, la comparación constante de marcos regulatorios y el fortalecimiento de mecanismos regionales de adecuación, para facilitar las transferencias internacionales sin comprometer los derechos de los titulares de datos.

En primer lugar, entender que una armonización legislativa a nivel global requiere esfuerzos no sólo de índole técnica sino también política, donde se logre alinear al objetivo de facilitar la protección de datos personales de los titulares de datos, sin perder de vista que muchos países tendrán mayor interés en restringir o dificultar el flujo de datos a ciertos países, viéndose traducido inclusive en bloqueo de páginas web o servidores de procesamiento.

En segundo lugar, el escenario global hoy resulta un tanto utópico por razones logísticas y hasta geopolíticas. En este contexto cada autoridad que pretenda mantenerse dentro del flujo internacional de datos personales, o entendiendo en términos de relación fundamental, realizando negocios variados a nivel internacional, es fundamental que comience a intentar a adecuar su normativa local a los estándares globales existentes, cubriendo con esto dos posibilidades. Por un lado, y si la armonización acaba realizándose bajo el faro del RGPD,

aumentando la lista de países considerados adecuados, lo cual facilitaría la realización de transferencias internacionales de datos personales sin necesidad de utilizar mayor cuerpo normativo que un *Data Processing Agreement* en los términos del artículo 28 del RGPD. Por el otro, si eso no fuese posible, aunque los cuerpos normativos poseyeran diferencias entre ellos, sería más fácil establecer parámetros de comparabilidad, donde se sepa que cuerpos normativos específicos coinciden en ciertas variables, y poder contrastar las que resulten diferentes, para ahorrar recursos al negocio quien contrataría un equipo letrado no necesariamente tan diversificado, que pueda cubrir lineamientos generales de los requisitos legales en los países involucrados. La contracara sería el caso de Estados Unidos, con más de diecisiete cuerpos normativos incoados a la fecha, criterios contrapuestos intranacionales partiendo desde qué entienden por datos personales a proteger (caso de california al inclusive entender datos *business to business* sin contemplar excepción), hasta qué tipo de acuerdo se necesita para proteger las transferencias de datos personales, dentro y fuera del país.

En conclusión, la respuesta a la pregunta "¿regionalización o continuidad?", la imposibilidad actual de armonizar es evidente. Por lo tanto, la pregunta no debe entenderse como una elección excluyente. Como proyección futura, se propone continuar trabajando hacia una convergencia progresiva que combine la regionalización táctica con una armonización gradual de principios y criterios en un modelo híbrido, en el que se impulse ese tipo de regionalización para facilitar el análisis y la implementación, mientras se mantenga una continuidad estratégica hacia la convergencia global. Valorar el camino trazado por el RGPD, sin replicarlo mecánicamente, y adaptarlo a la realidad cambiante del tratamiento internacional de datos.

Sin embargo, a la luz del Dictamen analizado a profundidad, es menester no convertir una necesidad práctica cubierta a tiempo por parte del EEE, en una abstracción teórica pasible de convertirse en inaplicable con la complejidad que las transferencias internacionales poseen en la actualidad, en contraste con los requisitos excesivamente onerosos impuestos por la autoridad de aplicación. Solo de esta forma será posible construir una protección de datos que sea al mismo tiempo robusta, viable y sostenible.

Concluyendo entonces, puede decirse que avanzar hacia una armonización legislativa, incluso si es parcial o regional y sin representar grandes quiebres con el sistema existente, no sólo constituye una mejora técnica en materia de protección de datos desde un punto de vista jurídico-legal, sino que representa una condición necesaria y fundamental para fortalecer la seguridad jurídica, reducir la incertidumbre regulatoria y garantizar un entorno confiable y

previsible para el desarrollo de los negocios en la economía global actual. Se espera que el presente trabajo contribuya al debate doctrinario y práctico en materia de protección de datos personales, ofreciendo una perspectiva que promueva la convergencia progresiva entre regiones y la consolidación de un marco jurídico internacional más coherente y previsible.

En síntesis, los resultados del análisis confirman la hipótesis planteada y permiten alcanzar el objetivo general de evaluar la viabilidad de la regionalización como alternativa realista y estratégica frente a la imposibilidad de una armonización global inmediata.

VII- BIBLIOGRAFÍA CONSULTADA

BELLI, L., NOUGRÉRES, A., MENDOZA, J., PALAZZI, P., REMOLINA, N. (2023). Hacia un modelo latinoamericano de adecuación par la transferencia internacional de datos personales. Discussion paper presentado en la Computers, Privacy and Data Protection Conference Latin America (CPDP LatAm) 2023 para recibimiento de comentarios. La versión consolidada de este trabajo será publicada en "Protección de datos personales: doctrina y jurisprudencia. CETYS, CDYT, 2023, Buenos Aires. Recuperado de https://cpdp.lat/wp-content/uploads/2023/07/doc-discusion-cpdplatam23-2.3.pdf

BRANSEN, K. (2025) "*DOJ Finalizes Rule Prohibiting and Restricting Foreign Transfer of Personal Sensitive Data"* – EDUCAUSE REVIEW – Online – ProQuest - Recuperado de: https://www.proquest.com/openview/b70dd3e9a535e85b42ac6dcb61f5c29a/1?pq-origsite=gscholar&cbl=7213897

CHANDER, A. et Al (2021) "*Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation"*- Policy Research Working Paper 9594. World Bank's World Development Report 2021 Team in collaboration with the Macroeconomics, Trade and Investment Global Practice. Georgetown Law Faculty Publications and Other Works. 2374., Available at SSRN: https://ssrn.com/abstract=3827228 or http://dx.doi.org/10.2139/ssrn.3827228 - Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827228

Comisión Europea (2018). COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO. Mayor protección, nuevas oportunidades: Orientaciones de la

Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018. COM(2018) 43 final.

Comisión Europea (2017). *Article 29 Working Party. Adequacy Referential* (18/EN WP 254 rev.01).

CORRALES COMPAGNUCCI, M; ABOY, M. & MINSSEN, T. Cross-Border Transfers of Personal Data After Schrems II: Supplementary Measures and new Standard Contractual Clauses (SCC). *Nordic Journal of European Law*, *4*, Article 2. Recuperado de: https://doi.org/10.36969/njel.v4i2.23780

DE GUZMÁN PLASENCIA MEDINA, F. (2025) *"IA y privacidad: Armonización Normativa y Retos Regulatorios en la Unión Europea y España"* – Revista D'Internet Dret I Política – ISSN 1699-8154 – Recuperado de: https://raco.cat/index.php/IDP/article/view/432048/526844

DECISIÓN DE EJECUCIÓN (UE) 2019/419 DE LA COMISIÓN de 23 de enero de 2019 con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de Japón en virtud de la Ley sobre la protección de la información personal [notificada con el número C(2019) 304] (Texto pertinente a efectos del EEE) (2019).

DECISIÓN DE LA COMISIÓN de 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina (Texto pertinente a efectos del EEE) (2003/490/CE) (2003).

DECISIÓN DE LA COMISIÓN de 27 de diciembre de 2004 por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países [notificada con el número C(2004) 5271] (Texto pertinente a efectos del EEE) (2004/915/CE) (2004).

DECISIÓN DE LA COMISIÓN (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. Official Journal of the European Union.

DECISIÓN DE LA COMISIÓN de 5 de febrero de 2010 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del

Consejo [notificada con el número C(2010) 593] (Texto pertinente a efectos del EEE) (2010/87/UE) (2010).

DICTAMEN del Comité N° 22/2024 sobre determinadas obligaciones derivadas de la dependencia del (de los) encargado(s) y subencargado(s) del tratamiento. European Data Protection Board. Recuperado en fecha 11/5/2025 de https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202422_relianceonprocessors-sub-processors_es.pdf

Domenech, Juan J. G. (2018). Las decisiones de adecuación en el derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los Estados miembros. ISSN 1989-4570 - www.uc3m.es/cdt DOI: https://doi.org/10.20318/cdt.2019.4624

EUROPEAN PARLIAMENT (2021) Exchanges of Personal Data After the Schrems II Judgment - Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 694.678 – Recuperado de https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

GUTARRA, A. (2019). La teoría de la prohibición de regreso. Revista pensamiento penal. Recuperado en fecha 8/3/2025 de: https://www.pensamientopenal.com.ar/doctrina/47313-teoria-prohibicion-regreso

HONORABLE CÁMARA DE DIPUTADOS DE LA NACIÓN ARGENTINA - PROYECTO DE LEY - LEY DE PROTECCIÓN DE DATOS PERSONALES disponible en fecha 3/7/2025 en: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2025/PDF2025/TP2025/1948-D-2025.pdf

KUNER, C. (2017) "*Reality and Illusion in EU Data Transfer Regulation Post Schrems"* German Law Journal , Volume 18 , Issue 4 , 01 July 2017 , pp. 881 – 918 DOI: https://doi.org/10.1017/S2071832200022197 - Recuperado de https://www.cambridge.org/core/journals/german-law-journal/article/reality-and-illusion-in-eu-data-transfer-regulation-post-schrems/0341A0D14DC345730F9B48A496A968D3

KWIATKOWSKA, M (2019) *"Negotiating a data processing agreement: a practical perspective"* - Derecom: Revista Internacional de Derecho de la Comunicación y las Nuevas

Tecnologías, ISSN-e 1988-2629, Nº. 27 – Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=7064843

LÖNNBERG, C. (2025) "*Compliance Risks for EU Controllers The DPF Disproportionate Burden-Expense Exception and its Effects on EU Controllers' Duty to Provide a Copy of Personal Data via U.S. Processors"* – Tesis de Graduación – Master of Laws Program – Lund University - Recuperado de: https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9189189&fileOId=9197588

MAKSÓ, B. (2016). *"EXPORTING THE POLICY - INTERNATIONAL DATA TRANSFER AND THE ROLE OF BINDING CORPORATE RULES FOR ENSURING ADEQUATE SAFEGUARDS."* Pécs Journal of International and European Law, (II). Recuperado de https://journals.lib.pte.hu/index.php/pjiel/article/view/6871

MONTAÑO HURTADO, J et Al (2023) *"Impacto de la tecnología en la abogacía: cambios en la práctica legal en la era digital"* - Código Científico Revista de Investigación, 4(E1), 254-269 – Recuperado de http://www.revistacodigocientifico.itslosandes.net/index.php/1/article/view/96/197

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. (2020). Privacy Guide for Businesses: PIPEDA (Cat. No. IP54-94/2019E). Gobierno de Canadá. Recuperado de https://www.priv.gc.ca/media/2038/guide_org_e.pdf

ORTEGA GIMÉNEZ, A. (2017). Transferencia internacional de datos personales: del Safe Harbour al Privacy Shield. RLM nº4. Artículo nº 12. Recuperado de revistalexmercatoria.umh.es

ORTEGA GIMÉNEZ, A. (2024). ¿Y a la tercera va la vencida?... El nuevo marco transatlántico de privacidad de datos UE-EE.UU. Cuadernos de Derecho Transnacional (Marzo 2024), Vol. 16, Nº 1. Recuperado de https://e-revistas.uc3m.es/index.php/CDT/article/view/8432

PATTERSON, T. (2025) *"Cross-Border Cloud Data Transfers: Case Studies on Balancing U.S. Government Privacy Regulations with Global Business Needs"* – SSRN – Independiente http://dx.doi.org/10.2139/ssrn.5383863 - Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5383863

PHILLIPS, M (2018) "*International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)" Hum Genet* , 575–582 (2018). https://doi.org/10.1007/s00439-018-1919-7 - Recuperado de: https://link.springer.com/article/10.1007/s00439-018-1919-7#citeas

PIETRZAK, S. (2017) – "*TRANSBORDER DATA FLOWS: BINDING CORPORATE RULES AS A GLOBAL TRANSFER MECHANISM AND TRUSTED DATA PROCESSING AREA"* - Master Thesis Law and Technology LLM – Tilburg University – Recuperado de: https://arno.uvt.nl/show.cgi?fid=142708

RZAYEVA, J. (2024) - "*Standard Contractual Clauses as a GDPR safeguard: implementation and challenges"* - Vilnius University Faculty of Law - Department of Private Law – Recuperado de https://epublications.vu.lt/object/elaba:191367268/

REPUBLIC OF KOREA. (2023). *Personal Information Protection Act* (Act No. 14839, Amended 2023). Korea Legislation Research Institute. Recuperado de: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=62389&lang=ENG

SEGURA, P. (2019) *"A un año de Rodríguez contra Google: ¿Estableció la CSJN un derecho al olvido digital en Argentina?"* SAIJ - Recuperado de: https://www.saij.gob.ar/pablo-segura-ano-rodriguez-contra-google-establecio-csjn-derecho-al-olvido-digital-argentina-dacf150827/123456789-0abc-defg7280-51fcanirtcod?f=Total%7CFecha%7CEstado+de+Vigencia%5B5%2C1%5D%7CTema%2FDerecho+constitucional%5B3%2C1%5%20n%5B5%2C1%5D%7CTribunal%5B5%2C1%5D%7CPublicaci%20n%5B5%2C1%5D%7CColecci%20n+tem%20tica%5B5%2C1%5D%7CTipo+de+Documento%2FDoctrina&o=1&t=2797

SHI, P. et Al (2021) *"Governance of Privacy Protection: How Laws Will Be Adopted to Address New Technologies?"* - 23rd Biennial Conference of the International Telecommunications Society (ITS): "Digital societies and industrial transformations: Policies, markets, and technologies in a post-Covid world", Online Conference / Gothenburg, Sweden – Recuperado de https://www.econstor.eu/handle/10419/238053

SOBRINO GARCÍA, I. (2021). Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y Estados Unidos. Revista de Derecho Comunitario Europeo. Recuperado de https://www.cepc.gob.es/sites/default/files/2021-12/3931807sobrino-garcia.html

VACA-ALDÁS, J. et Al (2025) *"Protección de datos personales en la gestión de justicia análisis del marco normativo ecuatoriano frente a los estándares internacionales"* - 593 Digital Publisher CEIT, ISSN-e 2588-0705, Vol. 10, Nº. 3, 2025 - Universidad Bolivariana del Ecuador - Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=10287447

WOLFF, J et Al (2021) "*Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020"* Journal of Information Policy - https://doi.org/10.5325/jinfopoli.11.2021.0063 – Recuperado de https://scholarlypublishingcollective.org/psup/information-policy/article/doi/10.5325/jinfopoli.11.2021.0063/291999/Early-GDPR-Penalties-Analysis-of-Implementation