Universidad de San Andrés

Facultad de Derecho

Maestría en Derecho de los Negocios

Tesis Final

"La creación de un marco normativo internacional como posible solución a los dilemas que enfrenta la protección de datos personales"

Mariano Peruzzotti

DNI 27.282.135

Director de Tesis: Pablo Palazzi

Ciudad de Buenos Aires, 30 de Septiembre de 2023

Abstract

En el presente trabajo se analizan los problemas actuales en materia de protección de datos personales producto de la evolución legislativa y reglamentaria que ha tenido la disciplina a lo largo de los últimos años. También se desarrolla la posibilidad de encontrar una solución por vía de un marco normativo internacional que resuelva estas tensiones. Asimismo, se describen las iniciativas supranacionales que han sido tenido lugar a la fecha para luego trazar los lineamientos de un posible estatuto global que intente brindar respuestas a los desafíos existentes en materia de protección de datos personales.

Índice

I. Introducción. 3
II. Los problemas actuales que enfrenta la protección de datos personales. 6
II.A. La proliferación de marcos normativos locales. 7
II.B. Alcance extraterritorial de las normas de protección de datos. 11
II.C. Restricciones a la transferencia internacional de datos. 17
III. Iniciativas de marcos supranacionales. 22
III.A. Las Directrices de la OCDE. 25
III.B. Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico. 27
III.C. Convenio 108. 28
III.D. El RGPD. 29
III.E. Los Estándares de la Red Iberoamericana de Protección de Datos Personales. 30
III.F. Reflexiones sobre los cuerpos normativos existentes. 31
IV. Propuesta de un marco legal internacional. 32
IV.A. Observaciones preliminares. 32
IV.B. Consideraciones generales sobre un posible marco legal internacional. 33
IV.C. Elementos esenciales del acuerdo global. 37
IV.C.1. Definición de datos personales y datos sensibles. 38
IV.C.2. Principios de procesamiento de datos. 39
IV.C.3. Bases legales para el procesamiento de datos. 41
IV.C.4. Obligación de transparencia. 42
IV.C.5. Derechos de los titulares de datos. 44
IV.C.6. Obligaciones de seguridad. 47
IV.C.7. Evaluación de impacto en materia de protección de datos. 49
IV.C.8. Confidencialidad y transmisión de datos personales. 50

IV.C.9. Cooperación. 51
IV.C.10. Comentarios finales sobre los elementos de la propuesta. 53
V. Desafíos que surgen al avanzar hacia la privacidad global. 53
VI. Conclusiones. 55

I. Introducción.

El tratamiento de la información ha experimentado un crecimiento exponencial en los últimos años. Su importancia en la era actual es determinante producto de la globalización, la innovación y los avances tecnológicos. Esta revolución digital constituye uno de los hitos más paradigmáticos de la historia de la humanidad y que tiene la característica de impactar transversalmente a todas las actividades de nuestra sociedad.

En este contexto, los datos personales se han convertido en el combustible que impulsa la era digital. El valor significativo actual de la información personal es indudable. Los datos personales son una de las principales fuentes de valor de muchas actividades comerciales modernas. En este sentido, la mayoría de las empresas actuales utilizan la información personal de sus clientes para incrementar sus ventas. A modo de ejemplo, el procesamiento de datos de los consumidores permite a los proveedores determinar los hábitos, necesidades e intereses y, en consecuencia, mejorar y personalizar sus servicios de acuerdo con las preferencias de cada uno de ellos. Asimismo, el sector público también se nutre de los datos de los ciudadanos para lograr una administración más efectiva y eficiente. No podemos negar tampoco que inclusive los partidos políticos emplean los datos personales de los ciudadanos para diseñar sus campañas electorales. Podríamos seguir enumerando ejemplos de actividades que se benefician de los usos de la información pero lo que es claro es que hoy en día casi todas las transacciones e interacciones sociales implican el tratamiento de datos personales.

Sin lugar a duda, el avance tecnológico implica un cambio sustancial en el enfoque de las cuestiones de protección de datos personales. La revolución digital ha generado la necesidad de poner a la privacidad en el centro de atención, promoviendo varias iniciativas destinadas a proteger la información personal.

Sin embargo, esa tendencia no ha sido uniforme en todo el mundo; tal es así que el desarrollo de la disciplina ha sido dispar en los diferentes países. Actualmente la protección de datos personales está sujeta a innumerables marcos normativos locales. De hecho, a pesar de que esta disciplina ha sido objeto de regulación en un número cada vez mayor de legislaciones domésticas durante los últimos años, todavía hay varios Estados que carecen de un régimen legal integral.

En términos generales, los principales propósitos de las leyes de protección de datos promulgadas localmente son garantizar la privacidad, la dignidad, el honor, la reputación y la autodeterminación informativa[1]. Si bien los principios fundamentales de alto nivel de las leyes de protección de datos parecen coincidir en la mayoría de las regiones y sistemas legales, las particularidades de los plexos normativos difieren sustancialmente. Naturalmente, estas diferencias son consecuencia de la diversidad cultural, social, económica y política de cada comunidad. Como tal, estos enfoques regulatorios divergentes conducen a un contexto legal altamente fragmentado y complejo con niveles desiguales de protección.

Se ha afirmado que la existencia de regulaciones en conflicto es una situación normal cuando falta una estructura legal jerárquica que pueda proporcionar un marco de gobernanza general[2]. De hecho, este pluralismo legal a nivel internacional condujo a iniciativas que buscaron armonizar las leyes de privacidad y protección de datos en todo el mundo. Sin embargo, hasta la fecha no ha salido a la luz un marco legal integral y comprehensivo sobre esta temática.

El impacto de una tecnología en creciente desarrollo y un procesamiento cada vez mayor de datos personales exige una respuesta urgente destinada a abordar estos problemas. En este sentido, la globalización y los avances tecnológicos propiciaron un crecimiento exponencial del fenómeno de Internet, lo que supuso un cambio global paradigmático tanto en el ámbito económico como social. Como tal, este nuevo panorama

[1] KUNER. "Data Protection Law and International Jurisdiction on the Internet (Part 1)", *International Journal of Law and Information Technology*, Vol. 18 No. 2, Oxford University Press, 2010, p. 177. (https://doi.org/10.1093/ijlit/eaq002; última consulta: 20 de septiembre de 2023).

[2] KUNER, "The European Union and the Search for an International Data Protection Framework*", Groningen Journal of International Law*, Vol. 2, Ed. 1: Privacy in International Law, 2014, p. 66. (http://www.kuner.com/my-publications-and-writing/untitled/kuner-groningen-journal-von.pdf; última consulta: 20 de septiembre de 2023).

no solo transformó los modelos de las empresas modernas, sino también la interacción entre las personas.

Al difuminarse los límites físicos de las diferentes jurisdicciones, Internet permitió la expansión del alcance de las empresas modernas y la conexión continua entre individuos a pesar de su ubicación geográfica. Naturalmente, el auge del comercio electrónico internacional representó también un aumento en el flujo de datos personales transfronterizo, lo que generó controversias sobre la privacidad de los datos teniendo en cuenta que los estatutos legales promulgados a la fecha son locales o, a lo sumo, regionales. Dado que la ley de protección de datos es, en general, aplicable cada vez que se procesan datos personales, puede aplicarse a casi cualquier operación realizada en Internet[3].

Además, el enfoque adoptado por los supervisores locales de protección de datos y los tribunales nacionales ha cambiado en los últimos años[4]. Las autoridades locales tienden a extender el alcance de sus leyes de protección de datos locales a jurisdicciones extranjeras de manera tal de lograr que los datos personales de sus ciudadanos se encuentren protegidos inclusive fuera de las fronteras de su propio territorio nacional. Dada la disparidad de criterios y niveles de protección legal existente entre los países, no es extraño que las autoridades nacionales reclamen un alcance extraterritorial de sus leyes al pretender aplicarlas en aquellos casos en los que la información personal de sus nacionales podría verse comprometida. Las autoridades han interpretado ampliamente los conceptos e institutos de sus propias normas de protección de datos, lo que ha llevado a extender su alcance jurisdiccional, dando lugar a un número significativo de disputas jurisdiccionales[5].

Los problemas actuales en materia de privacidad también derivan de las dificultades que las empresas globales deben atravesar para cumplir con múltiples leyes

[3] KUNER. *International Journal of Law and Information Technology*, 2010, p. 176.
[4] En este sentido vale mencionar las decisiones adoptadas por el Tribunal de Justicia de la Unión Europea en el caso Google Spain SL y Google Inc. v Agencia Española de Protección de Datos (AEPD) y Mario Costeja González (Caso C-131/12). También merece señalarse la decisión de la Agencia de Acceso a la Información Pública de Argentina que adoptó un criterio similar en el caso "Giolito c. Google Argentina SRL y Google LLC - EX-2019-84609512- -APNDNPDP#AAIP", disponible en https://www.argentina.gob.ar/sites/default/files/rs-2020-25457045-apn-aaip_google.pdf. (última consulta: 20 de julio de 2023).
[5] KUNER. *International Journal of Law and Information Technology*, 2010, p. 177.

de protección de datos promulgadas en todo el mundo. En este sentido, el pluralismo legal y la naturaleza transfronteriza de las organizaciones modernas, las cuales tienden a abarcar varias jurisdicciones, también ha generado inconvenientes prácticos a la hora de poder adaptar procesos que se encuentren alineados a las distintas obligaciones referidas a protección de datos personales.

Estos problemas que atraviesa privacidad conllevan importantes implicancias, ya que pueden disuadir a las personas y empresas de participar en el comercio electrónico, pueden resultar inquietantes para las personas cuyos datos personales se procesan e imponer cargas a las autoridades de protección de datos personales[6]. Ciertamente, este escenario constituye no solo un factor desalentador para las inversiones de las empresas sino que también puede generar una disminución en el nivel de protección de la información personal y, consecuentemente, de la confianza de los titulares de datos.

En base a lo expuesto, resulta necesario trazar alternativas y propuestas que tiendan a resolver estos dilemas. En ese contexto, se plantea la necesidad de considerar el desarrollo de un marco legal internacional sobre protección de datos personales que pueda erigirse como una alternativa valiosa para abordar las preocupaciones en materia de protección de datos personales planteadas anteriormente. La idea que se esboza en este trabajo, es decir, la creación de un instrumento legal supranacional que brinde soluciones a dichos conflictos, se orienta a lograr ese objetivo. Siendo consciente de las dificultades que puede conllevar la negociación de tal documento, entiendo que éste podría ser una posible opción para la resolución de las preocupaciones relativas a la protección de datos personales que se plantean actualmente.

II. Los problemas actuales que enfrenta la protección de datos personales.

Como se ha señalado en la introducción, la protección de datos personales enfrenta desafíos derivados de la coexistencia de distintos sistemas normativos que no son armónicos entre sí. Estos plexos normativos discordantes son producto de distintas tradiciones jurídicas que han generado un desarrollo desigual de la disciplina.

[6] KUNER. *International Journal of Law and Information Technology*, 2010, p. 178.

Por otro lado, vemos una constante vocación de los Estados a través de sus legisladores, autoridades nacionales y tribunales de extender el alcance extraterritorial de sus leyes. En los siguientes apartados se analizará este complejo escenario en el que se desarrolla la protección de los datos personales en la actualidad.

II.A. La proliferación de marcos normativos locales.

En los últimos años distintos países han sancionado leyes en materia de privacidad y protección de datos personales. Si bien existen aún jurisdicciones que carecen de normativa específica, lo cierto es que la tendencia demuestra que los Estados, conscientes de los desafíos y peligros que entraña el uso de las tecnologías en lo referido al resguardo de la privacidad, suelen inclinarse por regular esta cuestión. En ese sentido, la lista de países que ya cuentan con leyes comprehensivas en materia de protección de datos se va incrementando día a día.

En términos generales, los principales propósitos de las leyes de protección de datos promulgadas a nivel local han sido garantizar el resguardo integral de la privacidad e intimidad, el honor, la honra, la dignidad y la reputación. Si bien los principios fundamentales que recogen estos textos son similares en prácticamente todas las regiones, las particularidades de los marcos normativos difieren sustancialmente en algunos casos. Naturalmente, estas diferencias derivan de las características culturales, históricas, sociales, económicas y políticas propias de cada comunidad. Como tal, estos enfoques regulatorios divergentes conducen a un contexto legal altamente fragmentado y complejo con niveles desiguales de protección de los datos personales.

Si bien los principios generales en materia de protección de datos personales que fueron adoptados por las legislaciones nacionales y regionales contienen muchos puntos en común, su interpretación y aplicación en jurisdicciones específicas difieren sustancialmente. A pesar del creciente reconocimiento internacional de la protección de datos, todavía existen diferencias considerables en los enfoques en todo el mundo debido a factores culturales, históricos y legales[7]. Esta naturaleza heterogénea de la normativa de protección de datos es un mero reflejo de las diferencias naturales sociales, económicas

[7] KUNER. *Groningen Journal of International Law*, 2014, p. 59.

y políticas propias de cada Estado. Ello claramente representa un desafío sustancial para las organizaciones.

Se puede decir que hay dos modelos regulatorios diferentes en materia de protección de datos personales producto de las posiciones adoptadas por los Estados Unidos, por un lado, y la Unión Europea, por el otro. Se han generado dos tendencias principales a nivel internacional que han enfatizado la brecha en el entorno de la protección de datos a nivel global.

Las distintas visiones consisten esencialmente en tener una percepción disímil acerca de la naturaleza de la protección de los datos personales en sí. Mientras que en Europa la protección de datos personales es reconocida como un derecho fundamental y es responsabilidad del Estado tomar todas las medidas de tutela necesarias, los Estados Unidos consideran que la privacidad es un bien susceptible de ser transado y, como tal puede ser canjeado por beneficios económicos[8]. En otras palabras, los Estados Unidos valora la privacidad como un activo, es decir, un derecho económico que constituye parte de la propiedad de un individuo y que, como tal, puede negociarse en el mercado. La Unión Europea, por su parte, califica la privacidad de los datos como un derecho fundamental inherente a cada individuo y, en consecuencia, inalienable.

Esta diferente percepción sobre el derecho a la privacidad dio lugar a la adopción de distintos modelos de legislación. En este sentido, mientras que el marco legal de protección de datos personales de la Unión Europea se ha conformado en un estatuto único y completo, Estados Unidos ha implementado leyes y regulaciones de protección de datos específicas para cada sector, además de legislación de nivel estatal[9].

La privacidad de los datos de los ciudadanos europeos se protege principalmente a través del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al

[8] ALO. "EU Privacy Protection: A Step Towards Global Privacy", *Michigan State International Law Review*, Vol. 22.3, 2014, p. 1115. (https://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?article=1155&context=ilr; (última consulta: 30 de septiembre de 2023)

[9] KUDOS. *EU Versus US Privacy Legislation – Convergence?* Disponible en sitio: https://www.kudos-data.com/eu-versus-us-privacy-legislation/; (última consulta: 30 de septiembre de 2023).

tratamiento de datos personales y a la libre circulación de estos datos (en adelante, "RGPD"). Previo al RGPD, Europa había aprobado la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos; regulación que persiguió la armonización de los textos normativos dentro del bloque comunitario y, al mismo tiempo, crear condiciones básicas de protección de la información personal de los ciudadanos europeos. De esta forma, Europa adhirió a un sistema de regulación horizontal en el sentido de tener una ley que abarque a toda actividad de procesamiento de datos sin importar la industria o sector específico.

Por su parte, la privacidad de los datos de los ciudadanos estadounidenses está protegida a través de múltiples leyes, dependiendo del Estado en cuestión y la naturaleza de los datos involucrados en las actividades de procesamiento. Por ejemplo, el tratamiento de los datos relacionados a la salud está regido por la Ley de Portabilidad y Responsabilidad del Seguro Médico, comúnmente conocida como HIPAA por sus siglas en ingés, mientras que los datos financieros se rigen por la Ley Gramm-Leach-Bliley. No existe un cuerpo único federal que abarque todas las industrias o actividades, ya que se adopta un modelo de regulación vertical o sectorial.

Sin embargo, las regulaciones promulgadas recientemente como la Ley de Privacidad del Consumidor de California, conocida como CCPA por sus siglas en inglés, muestran una posible nueva tendencia dentro de los Estados Unidos que podría significar un cambio de enfoque gradual en el sentido de adoptar una visión más integral de la protección de datos personales que se pueda asemejar, en cierta forma, a la Unión Europea. No obstante, y aun cuando existan voces que promuevan su discusión, es importante aclarar que la sanción de una ley federal comprehensiva en materia de protección de datos personales en dicho país se encuentra aún hoy en un estado embrionario.

El análisis no debe limitarse a la situación de los Estados Unidos y Europa. En el mundo existen actualmente una gran cantidad de marcos normativos que atienden el fenómeno de la protección de datos personales. Sin ir más lejos, en Latinoamérica muchos Estados han sancionado estatutos legales en los últimos años, tal como Argentina, Brasil, Colombia, México, Uruguay, Perú, Costa Rica, Nicaragua, República Dominicana,

Panamá, Barbados, El Salvador, Ecuador, Cuba, Paraguay y Chile. Adicionalmente, otros países se encuentran discutiendo la sanción de leyes como es el caso de Bolivia y Honduras.

En otras latitudes nos encontramos con el mismo escenario. A modo de ejemplo, China sancionó su ley de protección de datos personales hace pocos años y la India se encuentra dando sus últimos pasos en la promulgación de su texto normativo. Australia, Nueva Zelanda, Japón y Corea del Sur también poseen leyes que regulan la información personal, lo mismo que Israel y muchos otros países en el mundo.

Esta dispersión de estatutos legales, cada uno de ellos con sus características y rasgos propios, genera un complejo entramado que, en ciertos supuestos, puede derivar en conflictos de normas. En los casos en los que apliquen simultáneamente a un mismo tratamiento de datos dos o más cuerpos normativos, la superposición de institutos con visiones y características distintas, genera un estado de incertidumbre que afecta a los sujetos involucrados, sean titulares de datos, responsables o encargados de tratamiento e inclusive a las autoridades locales.

Este fenómeno ha derivado en que las empresas deban enfrentar dificultades prácticas a la hora de cumplir con múltiples leyes de protección de datos personales promulgadas en todo el mundo. En efecto, las organizaciones que operan en distintas jurisdicciones deben responder a un escenario regulatorio cada vez más complejo y desafiante en el que el cumplimiento de determinada legislación puede llevar a tener que desobedecer los estándares legales vigentes en otros países.

El creciente número de conflictos normativos provocados por las diferentes concepciones nacionales y regionales de la protección de datos, como ilustra la sentencia del 6 de octubre de 2015 del Tribunal de Justicia de la Unión Europea en el caso

comúnmente denominado Schrems I[10], debería ser una llamada de atención para la comunidad internacional con respecto a esto[11].

Ciertamente, estas leyes presentan algunos elementos que conspiran contra una convivencia pacífica. En los siguientes acápites se analizarán puntualmente dos institutos existentes en muchas de las normas de protección de datos personales que sirven para ejemplificar la conflictividad normativa que enfrenta la disciplina actualmente: el alcance extraterritorial de las normas de protección de datos personales y la transferencia internacional de datos.

II.B. Alcance extraterritorial de las normas de protección de datos.

Una de las preocupación que ha generado la aprobación de marcos normativos locales es la tendencia emergente caracterizada por la inclusión, en muchos de los nuevos textos legales, de disposiciones que extienden su alcance territorial. En los últimos años han surgido distintas voces que, conscientes de las consecuencias del impacto producido por las tecnologías en un mundo cada día más interrelacionado y conectado, destacan la necesidad de repensar el enfoque territorial de la privacidad. En tal sentido, la creciente complejidad del procesamiento de datos realizado a escala mundial derivó en una reformulación del modo de analizar los conflictos relativos a la protección de datos. Es así como se plantea que el alcance global de una Internet que no conoce de fronteras requiere como respuesta una aplicación de la ley que tampoco se encuentre limitada por los márgenes territoriales[12].

De esta forma, aparece en escena la intención de los Estados de extender el alcance de sus normas extraterritorialmente. La Comisión de Derecho Internacional (CDI) define la "jurisdicción extraterritorial" como un intento de regular por medio de la legislación

[10] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA. "Maximillian Schrems v Data Protection Commissioner. Caso C-362/14." Sentencia del 6 de octubre de 2015. Disponible en https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 (última consulta: 24 de septiembre de 2023).

[11] KITTICHAISAREE, KUNER. *The Growing importance of Data Protection in Public International Law.* Publicado en EJIL:Talk! Blog of the European Journal of International Law, 2015. Disponible en https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/ (última consulta: 30 de septiembre de 2023).

[12] Peruzzotti, Mariano. 2020 "Alcance territorial de las leyes de protección de datos personales", *Revista La Ley*, 2020-F, Buenos Aires. Ed. Thomson Reuters La Ley, p. 428.

nacional, la adjudicación o la aplicación de la conducta de las personas, los bienes o los actos más allá de sus fronteras que afectan a los intereses del Estado en ausencia de tal regulación en virtud del derecho internacional"[13].

En este sentido, en los últimos años se han aprobado varias leyes locales que amplían el ámbito territorial de sus disposiciones. El artículo 3 del RGPD es un claro ejemplo de esta tendencia. En efecto, el RGPD extendió el alcance territorial de sus disposiciones de forma tal que comprenda actividades de tratamiento realizados fuera de las fronteras en las que rige la normativa comunitaria, inclusive cuando el agente se encuentra en extraña jurisdicción[14].

Las disposiciones del RGPD aplican a organizaciones establecidas en la Unión Europea como a aquellas que, ubicadas fuera del ámbito del bloque comunitario, realicen un tratamiento de datos que tenga un punto de conexión con Europa, ya sea porque ofrezcan productos o servicios a sujetos en la Unión o monitoreen comportamientos de individuos en tal región. Vemos así el reconocimiento expreso al alcance extraterritorial de las normas en materia de protección de datos.

Pero el RGPD no es el único cuerpo normativo que ha consagrado los efectos extraterritoriales de sus disposiciones. Es posible encontrar otros estatutos que han adoptado un enfoque similar, como es el caso de la Ley de Privacidad del Consumidor de California, la Ley General de Protección de Datos Personales de Brasil, la Ley de Protección de Datos Personales de Uruguay conforme su reciente reforma o la Ley Orgánica de Protección de Datos Personales de Ecuador, entre otros. Inclusive, los

[13] Reporte de Trabajo de la quintagésima octava sesión de la Comisión de Derecho Internacional, Anexo E, parágrafo 2 (2006). Disponible en https://legal.un.org/ilc/reports/2006/ (última consulta 30/9/2023).

[14] En tal sentido, el art. 3º establece lo siguiente:

"1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión,
independientemente de que el tratamiento tenga lugar en la Unión o no.

2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el derecho de los Estados miembros sea de aplicación en virtud del derecho internacional público".

proyectos de leyes de protección de datos que se discuten en varios países actualmente incluyen disposiciones en el mismo sentido, tal como en Argentina y Chile.

El RGPD, así como las normas que incorporaron una disposición similar, aumenta significativamente el ámbito de aplicación de la ley de forma unilateral. En la práctica, la consecuencia de este tipo de reglamentos es que la norma de origen prácticamente acompañará a los datos personales durante toda su vida y en todo tratamiento que se realice, tanto dentro de su territorio como fuera de él.

La aplicación de una norma con efectos extraterritoriales como el RGPD determina la necesidad de que un responsable o encargado de tratamiento deba cumplir con las distintas obligaciones que impone esa legislación, aun cuando no se encuentre radicado en el país donde rige tal cuerpo legal. Por ende, una organización que ni siquiera tenga sede, servidores o elementos de procesamiento de datos en un país, quedaría aun así sujeta a la norma que rija en tal lugar por el mero hecho de destinar esfuerzos comerciales en esa región.

Algunos juzgan positivamente la aplicación extraterritorial de la ley de protección de datos en tanto se erige como un mecanismo para proteger los derechos de las personas frente a amenazas fuera de la jurisdicción, mientras que otros, con una visión más crítica, la consideran una intromisión indebida de un Estado extranjero en los intereses nacionales.

El RGPD, así como todas las recientes leyes que reconocieron el alcance extraterritorial de sus disposiciones, supone una ampliación unilateral de la aplicación de la legislación a organizaciones extranjeras. Nadie podría negar ni desconocer que esta expansión se justifica por el dominio de una Internet sin fronteras, que en respuesta requiere también una aplicación de la ley que no conozca de límites territoriales. En cierto modo, no cabe duda de que una protección de datos eficaz en Internet no se lleva bien con un ámbito de aplicación nacional[15].

[15] AZZI, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation", *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 9 (2), 2018, p. 130. (https://www.jipitec.eu/issues/jipitec-9-2-2018/4723; última consulta: 30 de septiembre de 2023).

Fuera de todo juicio de valor, lo cierto es que los Estados parecen más preocupados en proteger a sus residentes del uso indebido de sus datos realizado fuera de las fronteras nacionales que en evitar conflictos jurisdiccionales con otros países. En consecuencia, se ha recurrido a adaptar bases jurisdiccionales que eran aplicables a otras áreas del derecho para resolver los temas de privacidad[16].

Claramente, no puede considerarse irrazonable que los Estados pretendan proteger los derechos de sus propios ciudadanos y residentes y, para ello recurran a fortalecer las garantías existentes, otorgar mayores derechos y establecer condiciones estrictas para el uso de los datos personales. Los nuevos marcos normativos apuntan, por un lado, a elevar el nivel de protección y, por el otro, evitar que ciertas actividades de procesamiento queden inmunes o ajenas al cumplimiento de las obligaciones respectivas. Es, en base a esto, que se exige a organizaciones que no tienen presencia en ese Estado someterse a su ley.

Esta solución tiene sentido desde el punto de vista del ejercicio de la potestad de control y del poder de policía de los Estados amén de un criterio de equidad. Aquellos establecimientos que pretenden hacer negocios en un mercado concreto deberán cumplir con la ley local vigente en el lugar de la misma forma que lo hacen aquellas organizaciones que podemos llamar nacionales o propias del país de origen. Consecuentemente, los Estados conceden un tratamiento igualitario tanto a las organizaciones locales como a las extranjeras, evitando concesiones favorables a entidades sin anclaje en el país que, por tal factor, puedan eludir atenerse al estatuto legal respectivo.

Por último, existe un argumento adicional para promover regulaciones que proponen un alcance extraterritorial cual es el factor disuasivo. Las empresas generalmente preferirán cumplir con la norma antes que tener que afrontar las consecuencias, aun cuando el *enforcement* extraterritorial sea poco probable o complejo. Los responsables o encargados no residentes no tendrán mayores incentivos en cometer conductas que puedan constituir un uso indebido de datos personales en tanto ello podría ser objeto de sanciones, que dicho sea de paso, cada día suelen ser más elevadas. A modo

[16] KUNER. "Data Protection Law and International Jurisdiction on the Internet (Part 2)", *International Journal of Law and Information Technology*, n. 3, vol. 18, 2010, p. 246.

de ejemplo, el RGPD impone multas administrativas máximas de Euros 20.000.000 o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía[17]. Las leyes que se promulgaron en otros países en los últimos años recogen ese criterio al imponer altas multas en casos de incumplimientos. También debe tenerse en cuenta que un infractor puede ser objeto de reclamos judiciales y tener que afrontar el pago de indemnizaciones por los daños y perjuicios que pudo haber ocasionado.

No obstante, los efectos extraterritoriales de las leyes de protección de datos generan inconvenientes considerables. En este sentido, la expansión del alcance de las regulaciones conduce a conflictos normativos.

La extraterritorialidad provoca la aplicación de múltiples leyes a un mismo caso, lo que representa un gran desafío para las empresas a la hora de cumplir con los requisitos locales en materia de protección de datos. Las organizaciones con actividades globales están sujetas a diferentes leyes locales cuyas disposiciones pueden no solo diferir sino que, en ciertos casos, incluso contradecirse. Por tanto, las dificultades a las que se enfrentan los responsables y encargados del tratamiento desde esta perspectiva son innegables, ya que en determinados casos el cumplimiento de una de las leyes aplicables puede conllevar el incumplimiento de otra ley incompatible pero también obligatoria.

En efecto, la proliferación de marcos normativos estrictos, repleto de extensas y complejas condiciones y obligaciones que deben atender las organizaciones, conspira contra el desarrollo de los negocios. De hecho, algunas reglas importan cargas administrativas complejas y gravosas que demandan cambios en las estructuras de los negocios. El RGPD ha marcado la agenda en este sentido. Además de extender extraterritorialmente sus disposiciones, ha propulsado un complejo marco normativo con una innumerable cantidad de obligaciones principalmente en cabeza del responsable del tratamiento, que en muchos casos significa un costo que para algunas organizaciones resulta muy difícil de poder afrontar.

[17] Artículo 83.6 del RGPD.

A modo de ejemplo, se ha dicho que parece absurdo que organizaciones no europeas con una interacción limitada con residentes de la Unión Europea deban implementar también medidas que podrían representar potencialmente un elevado costo administrativo como es el caso de la designación de un delegado de protección de datos. Esas reglas deberían aplicar solamente a los negocios que tengan una presencia sustancial en el mercado de destino, en este caso, el europeo[18].

En consecuencia, se genera un entorno caracterizado por la aparición y proliferación de marcos normativos sofisticados, exigentes en muchos aspectos y complejos en otros, sumado a la reivindicación de un alcance extraterritorial de las disposiciones. Todo ello conduce a un panorama altamente complejo y desafiante para las organizaciones que en muchos casos siquiera saben cómo afrontarlo, es decir, tener claro qué deben hacer para cumplir con todas las regulaciones a las cuales están sujetas o pueden llegar a estarlo.

Más allá de la carga que general el cumplimiento para las empresas extranjeras, por no hablar de los elevados costes de las multas administrativas, la reivindicación extraterritorial de las normas podría también considerarse un desafío a la soberanía estatal. Las discusiones sobre la aplicación exorbitante de las leyes de protección de datos se concentraron en gran medida en la determinación de una base teórica que ampare la extensión de su alcance sin reconocer que un régimen jurisdiccional siembre debe atender sus límites y fronteras. Si bien no es objeto de este trabajo profundizar sobre este eje, no es posible dejar de mencionar que la reivindicación extensiva que pretenda un Estado sobre actividades de procesamiento realizadas en otro país podría dar lugar a un conflicto jurisdiccional internacional, en particular en los casos en los que no exista algún tipo de colaboración o relación cordial entre ambas naciones.

A la luz de lo anterior, puede decirse que nunca antes se han esgrimido posiciones tan radicales en el reconocimiento extraterritorial de las disposiciones legales. Y es en este contexto que se genera un gran desconcierto producto de la superposición normativa que conspira contra la confluencia armónica de las legislaciones locales**.**

[18] SVANTESSON. "Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation". *International Data Privacy Law*, 2015. Vol 5, No. 4, p. 231.

II.C. Restricciones a la transferencia internacional de datos.

La mayoría de las normas de protección de datos personales, en particular el RGPD, incorporan previsiones específicas en materia de transferencias internacionales. Estas reglas en general disponen restricciones, condiciones y, en algunos casos, prohibiciones a la transmisión de datos personales a otros países. El propósito de estas regulaciones es extender el alcance de la protección de los datos aún después de que los datos hayan dejado el territorio de origen. Los legisladores, los tribunales así como los supervisores nacionales suelen tomar las medidas necesarias para evitar que los datos personales se vean privados de la protección que concede su legislación una vez transferidos fuera de su territorio. Aunque normalmente suele ser complejo emprender acciones coercitivas contra la entidad que trata los datos una vez que éstos se han transferido a un país extranjero, una autoridad de protección de datos puede requerir que el tratamiento en el extranjero se realice con arreglo a su propia legislación[19].

Algunas leyes pueden disponer la prohibición absoluta a la transferencia internacional, adhiriendo a una posición de soberanía extrema que no se condice con la realidad de los negocios y comercio internacional, el cual opera sobre la base de permitir la circulación transfronteriza de personas, mercancías, bienes, servicios y, lógicamente, también datos.

El criterio más extendido es aquel que permite la transmisión de datos sujeta a determinadas condiciones. En tal sentido, las leyes suelen disponer de mecanismos o resortes que habilitan esa transferencia.

En primer lugar, los estatutos legales tienden a autorizar la transferencia a jurisdicciones que posean legislaciones adecuadas, lo cual importa reconocer al país de destino un estatus de protección equivalente al del país de origen. Para esa determinación se suele emplear ciertos criterios o elementos que son considerados para analizar la situación específica de la jurisdicción en cuestión. En tal sentido, los parámetros que se evalúan suelen ser los siguientes: (i) el sistema normativo, tanto general como sectorial, incluyendo leyes sobre protección de datos personales, seguridad pública, defensa,

[19] KUNER. *International Journal of Law and Information Technology*, 2010, p. 181.

seguridad nacional y legislación penal; (ii) la aplicación de esa normativa; (iii) el acceso de las autoridades públicas a los datos personales; (iv) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes; y (v) los compromisos internacionales asumidos.

Aun cuando el país de destino no esté incluido en la lista de jurisdicciones adecuadas porque no llegue a cumplir las condiciones mencionadas, las normas suelen prever ciertos mecanismos que legitiman la transferencia, como es el caso de la suscripción de contratos de transferencia internacional, con cláusulas contractuales que en muchos casos son elaboradas por los reguladores o autoridades nacionales o supranacionales, así como las normas corporativas vinculantes.

Adicionalmente, las leyes también prevén supuestos en los cuales, excepcionalmente y bajo ciertas condiciones se habilita la transferencia internacional a países no adecuados, a saber: (i) cuando media consentimiento del titular del dato; (ii) cuando la transferencia sea necesaria para la ejecución un contrato o medidas precontractuales entre el titular del dato y el responsable del tratamiento; (iii) cuando haya un interés público comprometido; (iv) cuando sea necesario transmitir datos para proteger los intereses vitales del titular del dato o de otras personas, entre otros supuestos.

Cabe analizar el caso de las cláusulas contractuales. Estos documentos, tal como es el supuesto de las cláusulas contractuales estándar aprobadas por la Comisión Europea, suelen obligar a los importadores de datos ubicados fuera del Estado de origen de los datos (en este caso, la Unión Europea) a colaborar con las autoridades del país del exportador así como someterse a su autoridad del supervisor. Esto necesariamente representa la aplicación extraterritorial de la norma, lo que amplía su alcance y ámbito de influencia más allá de las fronteras geográficas del país de origen de los datos.

Más allá de eso, y aun cuando la comunicación de datos a un país determinado sea válida, las transferencias ulteriores estarán alcanzadas por las mismas condiciones o restricciones. Una transferencia ulterior se produce cuando los datos personales se transfieren lícitamente, es decir, mediante alguna de las alternativas que dispone la norma a una organización localizada en otro país, y a continuación, esa organización envía la información personal a un tercer Estado. Las autoridades de protección de datos

personales suelen considerar que las transferencias ulteriores deben tener una base legal ajustada al Derecho nacional aplicable del país desde el que se transfirieron originalmente los datos y, por ende, deben cumplir los requisitos básicos de la legislación respectiva. Siguiendo esta posición, la legislación del país de origen de los datos seguirá aplicándose a los datos personales que son objeto de transferencias ulteriores, a pesar de que los sucesivos países de destino de los datos posean normas específicas en la materia. En base a ello, la organización que realice ese tratamiento deberá velar por el cumplimiento de múltiples normativas, que inclusive podrían ser contradictorias entre sí.

Las iniciativas de reivindicación de la aplicación de la ley fuera de las fronteras territoriales buscan proteger los datos personales de nacionales y residentes con independencia del lugar del mundo en el que se traten. Esto hace inevitable que las regulaciones relativas a las transferencias internacionales de datos den lugar a conflictos con las legislaciones de los países a los que se exportan los datos, en particular cuando las normas no son consistentes. Esta problemática tiende a agravarse a medida que, en paralelo al crecimiento del comercio electrónico y la proliferación de nuevas tecnologías que no conocen de fronteras, los Estados y organizaciones regionales e internacionales adopten instrumentos jurídicos sobre protección de datos con restricciones a la transferencia internacional.

Los desafíos en materia de transferencia internacional se han exacerbado en los últimos años con motivo de los conflictos suscitados en Europa y derivados de la diferente actitud adoptada entre la Unión Europea y los Estados Unidos con respecto a los poderes de vigilancia otorgados a las autoridades gubernamentales locales con fines de seguridad pública y defensa nacional. Un ejemplo de ello es la histórica sentencia del Tribunal de Justicia de la Unión Europea en el caso que se ha dado en llamar Schrems II[20].

Mientras que los Estados Unidos otorgan amplios poderes de vigilancia a las autoridades gubernamentales con fines de seguridad pública y defensa nacional, al mismo tiempo restringe la capacidad de los ciudadanos extranjeros para hacer cumplir los derechos de privacidad. A ello hay que adicionar el enfoque divergente que se le ha dado

[20] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA. "Comisión de Protección de Datos contra Facebook Irlanda y Maximillian Schrems. Asunto C-311/18". Sentencia del 16 de julio de 2020. Disponible en https://curia.europa.eu/juris/liste.jsf?num=C-311/18 (última consulta: 29 de septiembre de 2023).

a la regulación en materia de protección de datos en los Estados Unidos en relación a la Unión Europea. Tal como se mencionó arriba, la Unión Europea ha adoptado un sistema de regulación horizontal a través del cual se aprobaron normas generales comprehensivas en materia de protección de datos personales que alcanzan a todas las actividades e industrias. Estas normas presentan restricciones a las transferencias internacionales de datos a países que no cuenten con leyes equivalentes. Los Estados Unidos se han caracterizado por adoptar un enfoque distinto en el sentido de que carecen de una ley federal comprehensiva en materia de protección de datos personales. Por ende, bajo la perspectiva de la Unión Europea y de todos los países que promulgaron regulaciones que siguen ese modelo, los Estados Unidos no son considerados un Estado que garantice un nivel de protección adecuado.

La ausencia de una norma federal ha sido el disparador para que ambos bloques tuvieran que negociar arreglos que permitieran la transmisión de datos. El primero de ellos dio lugar a los principios reconocidos como *Safe Harbor* o Puerto Seguro, adoptados por el Departamento de Comercio de los Estados Unidos; sistema que constituía un mecanismo de autorregulación al cual las empresas en ese país podían adherir voluntariamente, comprometiéndose a respetar ciertas reglas establecidas en su texto. La Comisión Europea declaró adecuado este sistema en el año 2000.

Maximilian Schrems inició una reclamación contra Facebook Irlanda por considerar que la plataforma social violaba los derechos de intimidad y protección de datos personales de los usuarios. Los datos eran transferidos desde Irlanda a servidores localizados en Estados Unidos, en donde eran procesados y utilizados por la red social Facebook. En Estados Unidos, los datos podían estar sujetos a un control estatal por parte de las agencias de investigación gubernamentales, lo cual constituía una práctica que podía afectar los derechos de los titulares de datos europeos.

La cuestión fue sometida a decisión (en cuanto a la interpretación del derecho aplicable) del Tribunal de Justicia de la Unión Europea. En el 2015 la Corte Europea declaró inválidas las transferencias internacionales a los Estados Unidos con base en el *Safe Harbor*. La anulación del *Safe Harbor* derivó en la necesidad de tener que acordar un nuevo mecanismo para legitimar las transferencias internacionales de datos. Las tratativas concluyeron en la aprobación del *Privacy Shield* consensuado por el

Departamento de Comercio de los Estados Unidos y las autoridades europeas. Este nuevo mecanismo fortalecía ciertos principios generales incorporados en el *Safe Harbor* y dotaba a los ciudadanos europeos de mayores resortes para resguardar sus derechos. En el año 2016 la Comisión Europea declaró que este mecanismo brindaba garantías adecuadas y, por ende, las transmisiones de datos a aquellas empresas certificadas bajo el régimen del *Privacy Shield* eran lícitas.

A raíz de la decisión adoptada por el Tribunal de Justicia de la Unión Europea y en el marco de la investigación iniciada por el regulador de Irlanda, Facebook Ireland explicó que una gran parte de los datos personales se transfería a Facebook Inc., basándose en cláusulas tipo de protección de datos. Consecuentemente, Schrems cuestionó, en particular, que el Derecho estadounidense obligue a Facebook Inc. a poner los datos personales que se le transfieren a disposición de las autoridades estadounidenses, como la *National Security Agency* (NSA) y la *Federal Bureau of Investigation* (FBI). Schrems también planteó que, al utilizarse esos datos en el marco de diferentes programas de vigilancia de una manera incompatible con las normas europeas, no se podía justificar la transferencia de esos datos a los Estados Unidos. En esas condiciones, el reclamante solicitó al regulador de Irlanda que prohibiese o suspendiese la transferencia de sus datos personales a Facebook Inc.

El caso llegó al Tribunal de Justicia de la Unión Europea, que dictó sentencia a través del cual legitimó las transferencias internacionales al amparo de las cláusulas contractuales tipo, pero, al mismo tiempo, declaró inválido al *Privacy Shield*[21]. En efecto, el tribunal dictaminó que los Estados Unidos no proveyeron un nivel adecuado de protección de los datos personales, y por lo tanto, las transferencias transfronterizas de datos personales entre dichas jurisdicciones sobre la base del Escudo de Privacidad no se ajustaban al derecho comunitario. Esto generó un gran trastorno para los negocios, especialmente para aquellas organizaciones que precisan del constante flujo transatlántico de datos.

[21] Peruzzotti, Mariano. "El caso Schrems II y sus implicancias en la región". Publicado en The Privacy Advisor. 4 de Agosto de 2020. Disponible en https://iapp.org/news/a/el-caso-schrems-ii-y-sus-implicancias-en-la-region/ (última consulta: 10 de abril de 2023).

Recientemente, los Estados Unidos y Europa negociaron un acuerdo transatlántico cuyo propósito es incrementar las garantías y protección de los datos personales de europeos de manera tal de habilitar una transferencia internacional de datos entre ambos bloques. Sin embargo, ya se han manifestado voces cuestionando su validez y anticipando que iniciarán las acciones legales respectivas para lograr su anulación[22], lo que, de lograrlo, generaría un mar de incertidumbre que pondría en riesgo claro y evidente las operaciones comerciales internacionales.

El caso Schrems es simplemente un claro ejemplo de la problemática que se deriva de la existencia de regímenes con estrictas normas relativas a la transferencia internacional. La misma circunstancia se da en otras latitudes cuando las regulaciones de los países exportadores e importadores de datos no guardan relación. Esto se traduce en obstáculos para el comercio internacional que en ciertas oportunidades son muy difíciles de sortear por parte de las organizaciones.

III. Iniciativas de marcos supranacionales.

El carácter global del tratamiento de datos ha suscitado un creciente interés en viabilizar la posibilidad de regular la protección de datos a escala internacional. Como se ha dicho previamente, el tratamiento de datos personales se ha convertido en una actividad clave tanto de las entidades del sector privado como del sector público. Por su parte, el desarrollo de Internet ha hecho posible que las empresas, los gobiernos y los particulares transfieran enormes cantidades de datos por todo el planeta con simplemente apretar un botón del teclado.

En este contexto, las soluciones locales que se traducen en normas estaduales con las características que se analizaron en el anterior capítulo no parecen ser las más efectivas para abordar la problemática actual. Esto se debe a múltiples razones, muchas de los cuales han sido mencionadas previamente. Sin intención de reiterarlas, merece destacarse que la proliferación de marcos normativos locales que difieren entre sí genera inconvenientes para varios sectores.

[22] Ver https://www.reuters.com/technology/eu-announces-new-us-data-transfer-pact-challenge-ahead-2023-07-10/.

En primer lugar, los individuos cuyos datos se transfieren habitualmente por todo el mundo, a menudo desconocen ante quién deben dirigir su pretensión para proteger sus derechos. Por su parte, las empresas deben lidiar con la falta de armonización legislativa que deriva, en algunas ocasiones, en conflictos normativos. Por último, las autoridades de protección de datos, muchas de las cuales carecen de recursos suficientes para llevar a cabo sus tareas, tienen que enfrentar cuestiones complejas relacionadas a casos con múltiples ramificaciones territoriales producto de las comunicaciones en un contexto de evolución tecnológica constante. Mientras ello sucede, los Estados siguen aprobando normativas que pretenden extender su alcance territorial fuera de las fronteras del propio Estado, tal como se ha desarrollado en el anterior capítulo. Por ello es preciso aventurarse en la consideración de un documento que permita trazar lineamientos que ayuden a resolver los conflictos existentes en la actualidad con una visión global y uniforme.

A la fecha, no existe un instrumento legal global que pueda dar solución a estos dilemas. A diferencia de otras áreas del derecho que presentan interés internacional, la protección de datos personales no ha sido objeto de regulación jurídica por un instrumento global. Los tratados sobre derechos humanos que incorporan previsiones sobre el derecho a la privacidad no suelen ser lo suficientemente comprehensivos como para ofrecer a los particulares un recurso directo en casos individuales. Además, los tratados de derechos humanos como la Declaración Universal de los Derechos Humanos de 1948 y el Pacto Internacional de Derechos Civiles y Políticos de 1966 que protegen el derecho a la intimidad o a la vida privada, no mencionan específicamente a la protección de datos. El único instrumento global publicado al día de hoy es aquel denominado “Lineamientos sobre registros de datos personales computarizados” que fue aprobado en el marco de las Naciones Unidas el 14 de diciembre de 1990 y que constituye un documento orientativo no vinculante.

Se han formulado proclamaciones tendientes a alcanzar un marco jurídico internacional sólido en materia de protección de datos. Por ejemplo, en 2005, la 27ª Conferencia Internacional de Comisarios de Protección de Datos de Protección de Datos y Privacidad emitió la “Declaración de Montreux”, en la que apelaba a las Naciones Unidas “a preparar un instrumento jurídico vinculante que establezca claramente y en detalle los derechos a la protección de datos y a la privacidad como derechos humanos

exigibles"[23]. Desde entonces, en otras instancias de la Conferencia Internacional se han adoptado resoluciones similares[24].

Algunas empresas también han hecho llamamientos de este estilo; por ejemplo, en 2007, Google pidió la creación de "normas mundiales sobre privacidad"[25]. Los grupos de la sociedad civil también han reclamado la elaboración de estándares globales[26]. En el año 2009, un grupo de trabajo formado por varias agencias de protección de datos y liderado por la Agencia Española de Protección de Datos emitió la "Resolución de Madrid"[27] que constituye una propuesta conjunta para un proyecto de estándares internacionales en materia de protección de datos personales. El propósito de este documento fue servir como punto de partida para la concreción de un instrumento internacional. Cabe señalar que Argentina, representada por la anterior Dirección Nacional de Protección de Datos Personales, participó de aquella iniciativa.

Al mismo tiempo se observa cierta intención no tan solapada de la Unión Europea de promover a nivel global su propio marco normativo, como por ejemplo el RGPD. El propósito detrás de esta iniciativa es exportar el modelo europeo a la mayor cantidad de países de modo tal que sirva de estándar a ser adoptado al momento de emprender tareas legislativas. El hecho de que muchos Estados hayan seguido el modelo europeo a la hora de redactar sus estatutos parece confirmar ese posicionamiento. A modo de ejemplo, la mayoría de las normas de protección de datos sancionadas en Latinoamérica comprueba esta tendencia.

[23] La Declaración de Montreux puede ser consultada en el siguiente sitio: https://globalprivacyassembly.org/wp-content/uploads/2015/06/montreux_declaration-Spanish.pdf (última consulta: 30 de septiembre de 2023).

[24] 35° Conferencia Internacional de Protección de Datos y Privacidad de Comisionados de Protección de Datos Personales. Resolución sobre el anclaje de la protección de los datos personales y la protección de la privacidad en el derecho internacional. 23 al 26 de Septiembre de 2013. El texto de la resolución puede ser consultado en el siguiente sitio: https://globalprivacyassembly.org/wp-content/uploads/2015/02/International-law-resolution.pdf (última consulta: 3 de septiembre de 2023).

[25] Ver Declaración disponible en el siguiente sitio: https://publicpolicy.googleblog.com/2007/09/call-for-global-privacy-standards.html. (última consulta: 30 de septiembre de 2023).

[26] Ver Declaración de privacidad de Madrid, Estándares para un mundo global. 3 de Noviembre de 2009. Disponible en el siguiente sitio: https://thepublicvoice.org/madrid-declaration/ (última consulta: 3 de septiembre de 2023).

[27] El texto puede ser consultado en el siguiente link: https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_en.pdf (última consulta: 30 de septiembre de 2023).

Se vislumbra así una doble faceta en la posición europea. Por un lado, el esfuerzo tendiente en lograr un marco normativo global y, por el otro, la propagación de su modelo como parámetro de legislación en todo el mundo. El involucramiento de la Unión Europea demuestra las tensiones inherentes en el desarrollo simultáneo de criterios globales. El interrogante que se plantea a raíz de este posicionamiento es si efectivamente lo que se intenta es llegar a un diálogo consensuado en la elaboración de un marco global o la mera imposición de principios provenientes de la legislación europea. Adelanto mi posición en el sentido de que, sin desconocer la influencia internacional que ha tenido la Unión Europea en la difusión de su modelo, inducir la adopción de un sistema puede no ser la solución que reconozca las características culturales, sociales y políticas de cada país. Eso, además, podría llegar a constituir un entorpecimiento en el diálogo tendiente a lograr un acuerdo global.

Para avanzar en el desarrollo de un marco internacional de protección de datos es necesario identificar anticipadamente los obstáculos y problemas que habría de afrontar así como las lecciones aprendidas en otros procesos de armonización legislativa. Sobre esto último me abocaré en los próximos párrafos, en los que se analizan algunos documentos supranacionales de los cuales se pueden tomar ciertas bases que sirvan de pilares de una propuesta de marco global de protección de datos personales.

III.A. Las Directrices de la OCDE.

La Organización para la Cooperación y el Desarrollo Económicos (en adelante, "OCDE"), asociación internacional cuya misión es diseñar mejores políticas para una vida mejor y promover políticas que favorezcan la prosperidad, la igualdad, las oportunidades y el bienestar para todas las personas, ha desarrollado en el año 1980 las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales (en adelante, las "Directrices"). Este instrumento constituye la piedra angular del trabajo de la OCDE en materia de privacidad y es reconocida como la norma mundial básica para la protección de datos.

Las Directrices representan una base sólida para construir una protección eficaz, lograr la confianza de las personas y también para desarrollar enfoques internacionales comunes sobre los flujos transfronterizos de datos. La OCDE declara promover un

enfoque holístico de la privacidad y la protección de datos y trabaja continuamente con países y expertos para evaluar los avances y ofrecer recomendaciones prácticas sobre la aplicación de las Directrices en el entorno digital actual[28].

Las Directrices no son vinculantes y fueron redactadas de una forma flexible de modo tal que permitan erigirse como la base para las iniciativas legislativas en los países que no posean marcos normativos sobre protección de datos. Ello, en tanto este cuerpo está conformado por una serie de principios que pueden ser luego complementados por la regulación nacional respectiva.

El documento incluye los siguientes principios: principio de limitación de recogida, principio de calidad de los datos, principio de especificación del propósito, principio de limitación de uso, principio de salvaguardia de la seguridad, principio de transparencia, principio de participación individual y principio de responsabilidad. Por su parte, las Directrices tienen un apartado específico con reglas generales sobre restricciones en el libre flujo de datos y otro capítulo sobre cooperación.

El propósito de las Directrices ha sido lograr un justo equilibrio entre la protección de la privacidad y los derechos y libertades individuales sin crear barreras al comercio y permitiendo el flujo transfronterizo de la información. Al ser un documento elaborado en el seno de la OECD, su alcance es más extensivo que los instrumentos regionales que se comentarán a continuación.

No obstante, lo cierto es que las características propias del documento hace que las Directrices, al igual que muchos de los documentos comentados debajo, sean muy generales y permitan una interpretación local que pueda no ser armónica. Por ende, su incorporación al derecho nacional daría lugar a divergencias sustanciales que es justamente lo que se intenta evitar con una ley internacional en materia de protección de datos. Esto, además de otros factores, desalientan la adopción de este texto como elemento de uniformidad internacional.

[28] Ver https://www.oecd.org/digital/privacy/ (última consulta: 29 de septiembre de 2023).

III.B. Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico.

Un ejemplo destacado de norma regional de protección de datos es el Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico (en adelante, el "Marco de Privacidad"). El Foro es una organización multilateral creada en 1989 con el fin de consolidar el crecimiento y la prosperidad de los países alrededor del Océano Pacífico y encargada de tratar temas relacionados con el intercambio comercial, la coordinación económica y la cooperación entre sus integrantes.

Este Foro desarrolló un conjunto de nueve principios de privacidad que sus miembros pueden aplicar voluntariamente en sus economías nacionales. El Marco de Privacidad tiene como objeto garantizar una protección efectiva de la privacidad y, al mismo tiempo, asegurar el comercio continuado y el crecimiento económico en la región. El Marco de Privacidad promueve un enfoque flexible para la protección de los datos personales en todas las economías que participan del Foro, evitando al mismo tiempo la creación de barreras innecesarias a los flujos de información[29].

Esos nueve principios se refieren a la prevención del daño a los titulares de datos, el deber de información, la limitación a la recolección de datos personales, la restricción a los usos de los datos, los derechos de los individuos relativos a la utilización y divulgación de la información, el deber de respetar la certeza e integridad de la información, las medidas de seguridad, el acceso y corrección a los datos y la responsabilidad demostrada.

La crítica que se ha ensayado a este instrumento es que no garantiza una adecuada protección de los datos personales en tanto los principios reconocidos son demasiado genéricos y ambiguos, poco precisos y sin el grado de detalle y rigurosidad requerido por las modernas legislaciones en la materia. Si confrontamos los principios con el RGPD o las leyes comprehensivas aprobadas en los últimos años vemos que el Marco de Privacidad claramente no logra satisfacer todos los recaudos. Por ende, y siendo que para muchos países la protección de datos personales constituye un derecho fundamental, es

[29] Ver https://www.apec.org/publications/2005/12/apec-privacy-framework (última consulta: 20 de junio de 2023).

poco probable que se considere que este plexo normativo proporciona un nivel de protección aceptable o adecuado. Además, las características propias del Marco de Privacidad lo convierten en un sistema que posee una base inestable que habilitaría que cada miembro del Foro interprete estos principios básicos de distinta forma. Ello podría derivar en la aprobación de leyes estaduales que sean contradictorias entre los propios Estados partes.

III.C. Convenio 108.

El Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal N° 108 del Consejo de Europa (en adelante, "Convenio 108") fue suscripto en 1981 en Estrasburgo con el objetivo de garantizar a las personas físicas el respeto de sus derechos y libertades fundamentales. Es el primer instrumento internacional de carácter vinculante que protege la privacidad individual contra abusos cometidos en la recolección y procesamiento de datos personales. La adhesión al Convenio 108 está abierto también a aquellos países fuera del continente europeo.

En virtud de este Convenio, las partes deben implementar las medidas necesarias en su legislación nacional para aplicar los principios que establece con el fin de garantizar el respeto en su territorio de los derechos humanos fundamentales de todas las personas en lo que respecta al tratamiento de datos personales. Hasta la fecha, 55 países, incluidos Estados no europeos como Argentina, Marruecos, México, Senegal, Túnez y Uruguay, han firmado este tratado y sus protocolos.

A pesar del creciente reconocimiento internacional de este instrumento y del interés por la posibilidad de que el Convenio 108 sirva de base para una norma internacional de protección de datos, hay tres razones por las cuales no ha llegado a transformarse en un marco normativo global y difícilmente lo sea a futuro. En primer lugar, es innegable que este documento está fuertemente inspirado en la posición europea, lo cual genera ciertas reservas. En efecto, el mero hecho de provenir de un órgano europeo, aun cuando no sea de la propia Unión Europea, ha desincentivado su adopción. Otras regiones pueden no sentirse cómodas en tomarlo como inspiración o, directamente, elegirlo como marco de regulación internacional.

Por su parte, el Convenio 108 esta abierto a la suscripción de Estados que cuenten con legislaciones que se ajusten a los postulados del propio instrumento. Ello desalienta la adhesión por parte de aquellos países que se encuentren en estadios embrionarios en el proceso de sanción de leyes en la materia.

Por último, el Convenio 108 también se caracteriza por haber sido redactado utilizando términos demasiado generales, aun cuando sea mucho más detallista que el Marco de Privacidad. Es decir, el Convenio 108 carece de un grado de sofisticación tal como el que proponen las normas comunes de protección de datos generadas en el ámbito de la Unión Europea. En tal sentido, los Estados Miembros de la Unión Europea podrían considerar la necesidad de ir por un estatuto que sea más preciso en cuanto a las reglas aplicables y que permitiese reducir los cortocircuitos e interferencias de armonizaciones contradictorias.

III.D. El RGPD.

Tanto la Directiva 95/46/CE del Parlamento Europeo y del Consejo como su sucesor, el RGPD, constituyen marcos normativos supranacionales que lograron, en el seno de la Unión Europea, establecer un sistema de protección armónico. El proceso de uniformidad legislativa se caracterizó por elevar los estándares de tutela como consecuencia de la decisión del bloque comunitario de reconocer a la protección de los datos personales como un derecho fundamental.

Las normas comunitarias europeas han influido considerablemente en la promulgación de estatutos de protección de datos en otros Estados. En efecto, la Unión Europea ha hecho esfuerzos tendientes a que los países sin tradición propia de protección de datos personales aprueben leyes en la materia y, de hacerlo, se basen en su propio modelo. La política exterior de la Unión Europea orientada a tratar de fomentar la adopción de la legislación comunitaria como un aspecto del desarrollo del Estado de Derecho, incluida la financiación de proyectos de asistencia técnica que permiten a expertos en protección de datos de la Unión Europea trabajar con terceros países, han sido instrumentos de los que se ha valido aquel bloque regional para exportar su sistema.

La legislación de la Unión Europea se ha convertido en la norma a seguir en otras regiones por varias razones, como ser la simplicidad económica, los objetivos de adhesión, la conveniencia desde el punto de vista comercial y la importancia de la tutela de los derechos humanos. Los representantes de la Unión Europea utilizan a menudo la retórica de los derechos fundamentales para promover su sistema. Esta difusión jurídica sugiere incluso la existencia de una norma imperativa de protección de datos; sin embargo, no hay pruebas contundentes acerca de la existencia de una norma de este tipo, omnicomprensiva y ampliamente aceptada fuera del bloque comunitario europeo[30].

La determinación de la Unión Europea de exportar su modelo podría indicar una solapada intención de extrapolar los principios y reglas propias en un marco global. Cuantos más países adopten ese sistema más sencillo será lograr los consensos y aceptaciones para un cuerpo normativo internacional. Sin embargo, aun resta sortear un obstáculo importante que es lograr el convencimiento de los Estados Unidos sobre las bondades de este tipo de regulación horizontal, algo que parece no alinearse con su posicionamiento interno e internacional.

III.E. Los Estándares de la Red Iberoamericana de Protección de Datos Personales.

Distintas organizaciones han estado trabajando en la elaboración de estándares, lineamientos o recomendaciones internacionales en materia de protección de datos personales. Aun cuando no sean vinculantes, estos instrumentos han tenido un doble impacto: fomentar, por un lado, la promulgación de normas nacionales y, por el otro, tender vías para lograr la tan ansiada armonización legislativa producto de la sanción de normas que comparten un mismo espíritu.

En este marco, la Red Iberoamericana de Protección de Datos Personales, foro regional de Iberoamérica integrado por diversos actores, tanto del sector público como privado, elaboró y publicó en el año 2017 los Estándares de Protección de Datos Personales (en adelante, los "Estándares"). Los Estándares constituyen un conjunto de directrices orientadoras que contribuyan a la emisión de iniciativas regulatorias de

[30] TAYLOR. "The EU's human rights obligations in relation to its data protection laws with extraterritorial effect." *International Data Privacy Law,* 2015. Vol. 5, No. 4, p. 246, (https://academic.oup.com/idpl/article/5/4/246/2404460; última consulta: 30 de septiembre de 2023).

protección de datos personales en la región iberoamericana de aquellos países que aún no cuentan con estos ordenamientos, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes[31].

Argentina ha comenzado a transitar un proceso de reforma de su marco normativo sancionado en el año 2000. En tal sentido, los Estándares de la Red Iberoamericana han sido una de las fuentes de inspiración del Proyecto de Ley presentado por el Poder Ejecutivo de la Nación en el Congreso el 30 de junio de 2023, elaborado por la Agencia de Acceso a la Información Pública.

A diferencia de los instrumentos mencionados anteriormente, los Estándares se caracterizan por ser más concretos y específicos, brindando lineamientos bastante claros. En su texto se evidencia una impronta claramente europea en tanto la mayoría de sus disposiciones sigue los parámetros del RGPD. Esto se alinea con el posicionamiento que tuvo la región al escoger un sistema de regulación local.

III.F. Reflexiones sobre los cuerpos normativos existentes.

Como se ha analizado a lo largo de este capítulo, existen varios instrumentos internacionales que podrían servir, al menos en teoría, de base para un marco jurídico internacional de protección de datos. Entre ellos podemos mencionar el Convenio 108 o las Directrices. Sin embargo, es probable que factores políticos dificulten la reapertura de los instrumentos internacionales existentes para que sean utilizados como marco global. Además, no todos estos instrumentos son jurídicamente vinculantes[32] .

La alternativa sería elaborar un nuevo documento, como podría ser un convenio redactado por un órgano ad hoc compuesto por representantes de los Estados, del sector privado, expertos en la materia, asociaciones dedicadas a la privacidad y la sociedad civil, aun cuando ello conlleve tiempo y esfuerzo. En el siguiente capítulo se desarrollará esa propuesta de instrumento internacional.

---

[31] https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf (última consulta: 29 de septiembre de 2023).

[32] KUNER. "An International Legal Framework for Data Protection: Issues and Prospects", *Computer Law & Security Review*, Vol. 25, 2009, p. 24 y ss., (https://ssrn.com/abstract=1443802; última consulta: 30 de septiembre de 2023).

IV. Propuesta de un marco legal internacional.

IV.A. Observaciones preliminares.

Un marco legal internacional sobre protección de datos personales surge como una alternativa valiosa para abordar los conflictos sobre protección de datos en el entorno global y digital planteados en los anteriores párrafos. Este régimen ayudaría a lograr el establecimiento de un conjunto de principios y derechos comunes así como garantizar una protección legal equitativa de los derechos de titulares. También permitiría la simplificación del flujo de datos personales a través de los diferentes países y, en consecuencia, el desarrollo social y económico internacional; todo ello en un contexto que tienda a lograr la promoción de la cooperación internacional entre las autoridades locales. El primer incentivo de la armonización legislativa está relacionado con la reducción del impacto que generan las fronteras nacionales, lo que encuadra perfectamente con la motivación de muchos defensores de un marco internacional de protección de datos para facilitar el flujo de datos personales alrededor del mundo"[33].

Es innegable que entramos en un momento histórico en el cual resulta esencial discutir la posibilidad de resolver las discrepancias existentes y lograr los consensos para construir ese marco supranacional. Los textos normativos locales han derivado en escenarios en los que la inseguridad jurídica parecería haber prevalecido en ocasiones. Las crisis se han resuelto gracias a intervenciones *ad hoc* de las partes en conflicto que llegaron a acuerdos específicos para cada caso o debieron ser decididos por los tribunales. En párrafos anteriores se desarrolló el caso Schrems, el cual ha derivado en restricciones a los negocios internacionales e incertidumbre en cuanto a la forma de poder realizar las operaciones y actividades de tratamiento de datos. Por muy valiosas que hayan sido esas intervenciones y las lecciones aprendidas, tratar el problema caso por caso de poco sirve para mitigar la falta de seguridad jurídica a futuro, la cual, por cierto, presenta

[33] KUNER, *Computer Law & Security Review*. 2009, p. 12.

repercusiones económicas potencialmente gravosas. Por lo tanto, la necesidad de una solución global resulta imperativa[34].

No se escapa a este análisis que los enfoques legales divergentes adoptados a nivel local constituyen un férreo obstáculo a sortear. Esta situación plantea el interrogante de si las leyes actuales son compatibles entre sí y si esta forma de legislar localmente un medio sin fronteras e intrínsecamente internacional como es Internet es sostenible en el tiempo. Es indudable que por el propio imperio de la soberanía nacional, los Estados no van a renunciar a su potestad de regular el tratamiento de los datos personales, aspecto que tiene relevancia desde el plano de los derechos fundamentales así como elemento medular del negocio empresarial y de la actividad de las administraciones públicas. Pero ello no quita a que se intente buscar soluciones creativas a los conflictos existentes.

A pesar de las discrepancias significativas existentes en las leyes de protección de datos, considero que hay un principio de consenso en torno al conjunto de reglas básicas que viven en el corazón de la mayoría de las leyes nacionales y acuerdos regionales. Estas normas y principios generales podrían constituir el punto de partida para el desarrollo de un marco legal global que busque armonizar las numerosas legislaciones. Dado que estos principios recogen pautas básicas, podrían proporcionar una base sólida para un ordenamiento jurídico supranacional que establezca reglas generales que, en última instancia, puedan ser complementadas por la normativa local de cada Estado.

En los próximos párrafos se desarrollará esta premisa. No obstante, es importante señalar de antemano que para que esta propuesta tenga posibilidades ciertas de prosperar será esencial que las partes hagan concesiones recíprocas relativas a ciertos valores fundamentales, como el derecho a la autodeterminación informativa bajo el paradigma europeo o las garantías individuales y potestades gubernamentales bajo el sistema norteamericano.

IV.B. Consideraciones generales sobre un posible marco legal internacional.

[34] BOUGIAKIOTIS. "The Layered Links Model: An Alternative Approach to International Privacy Regulation", *International Data Privacy Law*, Vol. 10, Issue 3, 2020, p. 2, (https://ssrn.com/abstract=3464380; última consulta: 30 de septiembre de 2023).

Antes de proceder con el diseño de un instrumento global es preciso identificar cuatro temas de relevancia sustancial que exigen cierto consenso previo, a saber: (i) el enfoque o sistema a adoptar; (ii) el nivel de detalle que tendrá aquel marco; (iii) la organización a cargo de la tarea de redacción; y, por último, (iv) el tipo de instrumento a implementar. Ello es muy importante en cuanto a que no existe a la fecha siquiera acuerdo sobre qué debe entenderse concretamente por un tratado internacional en materia de protección de datos. A partir de la determinación de estos aspectos podrá luego estructurarse los institutos que nutrirán a ese instrumento global.

El primero de los temas mencionados se refiere al tipo de acuerdo que se precisará sobre el enfoque de privacidad a adoptar. Como se comentara en anteriores capítulos, hay dos tendencias principales en cuanto a la visión de la privacidad de datos expresadas en los modelos de los Estados Unidos y la Unión Europea. El correlato de ello es que la convivencia de estos sistemas, contradictorios en algunos aspectos, puede plantear algunos obstáculos a la hora de negociar un reglamento internacional.

Un análisis de las leyes de privacidad y protección de datos en todo el mundo revela que existe una tendencia creciente en seguir el sistema de regulación horizontal, que se expresa principalmente en el modelo europeo. No se puede desconocer que la normativa de la Unión Europea ha sido sumamente influyente al punto tal de constituirse en el estándar a seguir a la hora de redactar las leyes de protección de datos, especialmente en Latinoamérica.

Siendo que el sistema de legislación comprehensiva de carácter horizontal ha prevalecido en la mayoría de los países, pareciera que una interpretación flexible de los principios establecidos por el RGPD junto con un equilibrio adecuado entre las diferentes perspectivas locales podría servir como piedra angular de un estatuto internacional de protección de datos.

En segundo lugar, habrá que considerar el aspecto relativo al nivel de detalle que debe cubrir este marco legal. Si el estatuto internacional es demasiado abstracto, es posible que no pueda proteger los datos personales de forma efectiva. Por su parte, cualquier estándar que sea demasiado detallado puede ser difícil de implementar localmente teniendo en cuenta los divergentes sistemas regulatorios que existen en el

mundo actualmente.[35] Al momento, la mayoría de las iniciativas internacionales han formulado principios generales sin especificar como deben ser implementados. Por lo tanto, el verdadero desafío sería encontrar un balance que permita el equilibrio entre principios amplios que puedan ser lo suficientemente flexibles como para adaptarse a una variedad de escenarios locales y, al mismo tiempo, lo necesariamente exhaustivos para garantizar una protección adecuada de la privacidad en todo el mundo.

En tercer lugar, se debe determinar la institución que llevará a cabo la tarea de elaborar el marco normativo. Al respecto, se han ensayado algunas propuestas que van desde la Organización Mundial del Comercio hasta las Naciones Unidas. El clima politizado que existe actualmente en las organizaciones internacionales más reconocidas y la falta de una asociación internacional imperante en el campo de la protección de datos podría determinar que la mejor opción sería aquella a través de la cual se confíe la tarea a un grupo de trabajo ad-hoc. Si bien la Organización de las Naciones Unidas cuenta con las membresías globales necesarias considerando la cantidad de Estados parte, el trabajo de los órganos de armonización legal como la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (*United Nations Commission on International Trade Law*, "UNCITRAL") demuestra que en la atmósfera altamente politizada de esta organización, la armonización incluso de los temas técnicos tiende a avanzar lentamente y con dificultad. La Organización de las Naciones Unidas también carece de experiencia en el campo de la protección de datos personales[36].

Actualmente, ninguna organización internacional parece tener la combinación de alcance global, mandato para producir tratados internacionales y conocimiento en la regulación de protección de datos personales que sería necesaria. La experiencia ha demostrado que las iniciativas de armonización jurídica son bastante difíciles incluso en áreas técnicas del derecho y pueden serlo aún más en temas en los que existen profundas diferencias entre los Estados[37]. La creación de un comité específico integrado por representantes de diferentes jurisdicciones y partes interesadas que cuente con considerable experiencia en la materia podría ser una alternativa valiosa para la coordinación del instrumento supranacional.

[35] KUNER. *Groningen Journal of International Law,* 2014, p. 59.
[36] KUNER. *Groningen Journal of International Law,* 2014, p. 60
[37] KITTICHAISAREE. KUNER. *European Journal of International Law.* 2019.

Finalmente, la comunidad internacional debería acordar el tipo de instrumento de armonización que se adoptaría. Ello es una parte esencial del proceso de negociación para lograr un instrumento global. Hay muchas alternativas que podrían adoptarse como un tratado o convención multilateral, una ley modelo que los Estados pueden promulgar en sus estructuras legales nacionales, cláusulas o términos y condiciones que pueden ser incorporados en contratos y otros documentos celebrados entre particulares, normas no vinculantes, lineamientos internacionales, recomendaciones y códigos de práctica, guías legislativas, entre muchos otros. Como tal, cada enfoque de armonización posee sus fortalezas y debilidades[38].

La determinación del instrumento de armonización es una cuestión de suma importancia, ya que sin duda tendrá consecuencias en el logro de los fines previstos. Aunque han habido propuestas que giraban en torno a la utilización de un instrumento preexistente que sirviera de base para una armonización global, como podría ser el caso del Convenio 108, todo indica que las negociaciones de un marco legal completamente nuevo atraerían más atención y crearían incentivos para participar en las conversaciones.

A pesar de las ventajas que las alternativas no vinculantes, tales como los estándares de la industria, las guías internacionales, las recomendaciones y los códigos de práctica, entre otros, pueden proporcionar debido a su flexibilidad y adaptabilidad, la ausencia de aplicación gubernamental podría conducir a una baja tasa de implementación. Por lo tanto, estas herramientas no parecen ofrecer una solución integral y efectiva a los desafíos actuales.

Asimismo, una ley modelo también brindaría cierta flexibilidad en su implementación, lo que puede alentar a los Estados a decidir adoptarla. No obstante, esta flexibilidad probablemente derive en una deficiente armonización. Los Estados podrían diseñar su propio estatuto legal independientemente de los principios de la ley modelo considerando la ausencia de una sanción por no seguir un enfoque uniforme.

[38] KUNER. *Computer Law & Security Review*, 2009, p. 22.

Ciertamente, la alternativa de un tratado multilateral es la opción que garantizaría un mayor grado de armonización, ya que constituiría un texto único jurídicamente vinculante para todos los Estados miembros. Por supuesto que existen ciertas desventajas, inconvenientes o dificultades en la adopción de un arreglo multilateral. En este sentido podemos mencionar los siguientes obstáculos: (i) la potencial resistencia de los países a suscribir un instrumento vinculante; (ii) el tiempo y los costos financieros que demanden las negociaciones y la redacción del documento final; (iii) la posibilidad de que los Estados formulen reservas y derogaciones a determinadas disposiciones; y (iv) las dificultades para su futura modificación, cuando sea necesario considerando el transcurso del tiempo. Sin embargo, y a pesar de todo ello, entiendo que este tipo de instrumento permitirá acercarse al objetivo deseado, cual es lograr la armonización legislativa global que concilie un nivel adecuado de protección de los datos personales en todo el mundo y la concreción de los negocios comerciales.

En cualquier caso, es importante tener en cuenta que la uniformidad no está garantizada por la mera adhesión a un instrumento internacionalmente vinculante, sino que resulta y depende tanto de la aplicación nacional de este documento como de la interpretación que se realice de esa legislación en el ámbito nacional. La prueba de fuego se produce con la adopción real en la práctica y la aplicación por un tribunal nacional de una regla uniforme en una situación concreta[39].

Las leyes de protección de datos de los distintos países exponen principios básicos muy similares y comparten muchos puntos en común en cuanto a las pautas de aplicación. Sobre la base de ello se podría estructurar un marco global. En el siguiente capítulo se analizarán los elementos que componen la propuesta de un instrumento supranacional.

IV.C. Elementos esenciales del acuerdo global.

A continuación, se describen algunos principios que serían la base sobre la que se estructuraría la propuesta de un tratado internacional sobre protección de datos personales.

[39] KUNER. *Computer Law & Security Review*, 2009, p. 16.

IV.C.1. Definición de datos personales y datos sensibles.

En general, las leyes estaduales coinciden en el alcance del término "datos personales". En este sentido, los datos personales se definen como cualquier tipo de información relacionada con una persona física identificada o identificable, quien resulta ser el titular del dato personal. En otras palabras, un titular de datos personales es aquel que puede ser individualizado, directa o indirectamente, a través de un identificador, como el nombre, su carta o documento de identidad, datos de ubicación, etc. Por lo tanto, las disposiciones de las leyes de protección de datos personales solo se aplican a la información que está vinculada -o podría estar vinculada- a un sujeto determinado que generalmente es una persona humana aun cuando en algunos países se reconoce protección a las personas jurídicas, como es el caso de Argentina y Uruguay. Como consecuencia de ello, la información anonimizada –datos que no pueden atribuirse a persona determinada o determinable, o cuya asociación con una persona determinada o determinable es extremadamente compleja o requiere esfuerzos excesivos o desproporcionados– no entraría en el ámbito de las leyes de protección de datos personales.

En general, se entiende que cualquier tipo de información vinculada a una persona calificaría como dato personal. Por lo tanto, a modo de ejemplo, desde el nombre y los datos de contacto de una persona, hasta las imágenes, datos de geolocalización, información financiera o económica, hábitos de consumo o conducta y toda información que se relacione a una persona específica se considera como datos personales. El alcance de la definición es usualmente muy amplio.

Además, la mayoría de las leyes incorporan una categoría especial que se refiere a datos personales que están sujetos a regulaciones más rigurosas debido a su naturaleza sensible. En este sentido, comúnmente se propone un catálogo de datos que caen dentro de esta clasificación especial y que son objeto de un tratamiento preferencial en virtud de referirse a información relacionada con la esfera más privada e íntima del individuo. Un uso indebido podría exponer a ese individuo a un posible acto de discriminación.

Este tipo específico de datos generalmente incluye información personal que revela el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas,

afiliación sindical, datos genéticos, datos biométricos, datos relacionados con la salud y hábitos o comportamientos sexuales. Además, en algunas leyes los antecedentes penales están también sujetos a un tratamiento especial[40].

Cabe mencionar que existe cierta discrepancia en cuanto al alcance del término en algunas situaciones puntuales. Ciertas leyes consideran que la información financiera constituye un dato sensible, como es el caso de la información referida a los ingresos económicos de la Ley de Protección de Datos Personales N° 29.733 de Perú, mientras que otras no lo prevén, como es el caso del RGPD y la Ley de Protección de Datos Personales N° 25.326 de Argentina, entre muchas otras.

En base a lo expuesto, el tratado internacional incorporaría una definición amplia del término dato personal consistente con las legislaciones locales. También prevería un apartado específico para resguardar los datos sensibles.

IV.C.2. Principios de procesamiento de datos.

Las leyes de protección de datos generalmente se aplican a todo procesamiento de datos personales, es decir, abarcan cualquier operación o conjunto de operaciones que se realice con datos personales o conjuntos de datos personales, ya sea por medios automatizados o no, incluida la recopilación, almacenamiento, adaptación, divulgación, transmisión y destrucción de datos personales y, en general, cualquier gestión de datos personales[41]. Para encauzar esas actividades de procesamiento de datos y fijar reglas básicas, los estatutos legales suelen establecer principios generales.

Hay cierto consenso en los postulados generales reconocidos por la mayoría de las leyes así como en muchos de los instrumentos supranacionales mencionados en el

[40] A modo de ejemplo, el artículo 10 del RGPD dispone que el tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados.

[41] Existen algunas operaciones excepcionales de tratamiento de datos que, en general, no entran en el ámbito de aplicación de las leyes de protección de datos, como el tratamiento realizado en el marco de una actividad puramente personal o doméstica; el tratamiento realizado por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de delitos o de ejecución de sanciones penales; entre otras.

anterior capítulo. Es en base a ello el marco internacional debería estructurarse sobre la base de los siguientes principios fundamentales:

- Principio de licitud y transparencia: los datos recogidos deben obtenerse de forma lícita y tras haberle facilitado al titular de datos la información pertinente sobre las operaciones de tratamiento de datos. El tratamiento se considera lícito si se realiza conforme a lo establecido en el tratado internacional y leal si el responsable del tratamiento se abstiene de tratar los datos a través de medios engañosos o fraudulentos.

- Principio de finalidad: los datos recopilados solo deben utilizarse para fines compatibles con aquellos para los que se obtuvieron, excepto en el caso de operaciones de procesamiento particulares que no se consideren incompatibles con los propósitos iniciales (por ejemplo, procesamiento limitado a fines de archivo de interés público, fines de investigación científica o histórica; entre otros).

- Principio de minimización: los datos recopilados deben ser adecuados, relevantes y no excesivos en relación con el alcance y finalidad para la que se obtuvieron.

- Principio de exactitud y veracidad: los datos deben ser precisos y ser modificados o actualizados de manera oportuna siempre que sea necesario.

- Principio de limitación del almacenamiento: los datos recopilados deben ser eliminados inmediatamente cuando dejen de ser necesarios o actuales para los fines que motivaron su obtención, excepto para operaciones de procesamiento particulares, en cuyo caso pueden ser almacenados por períodos más extensos bajo condiciones de seguridad adecuadas.

- Principio de integridad y confidencialidad: los datos recabados deben ser tratados bajo estrictas medidas de confidencialidad y seguridad que aseguren su integridad.

- Principio de preeminencia: en caso de duda sobre la interpretación y la aplicación de la norma, prevalecerá la más favorable al titular de los datos personales.

- Principio de responsabilidad: el responsable y el encargado del tratamiento deben asumir la responsabilidad de cumplir con los principios y requisitos de protección de datos aplicables y mantener registros para demostrar dicho cumplimiento. A su vez, deben adoptar las medidas técnicas, organizativas o de cualquier otra índole que sean útiles, oportunas y efectivas con el fin de garantizar un tratamiento adecuado de los datos personales, el cumplimiento de las obligaciones dispuestas por el marco internacional y que permitan demostrar a las autoridades respectivas su efectiva implementación. Las leyes sancionadas en los últimos años han dispuesto una serie de medidas para cumplir con este principio que podrían ser recogidas por el tratado, entre las que se destacan las siguientes:
    - aplicar la protección de datos desde el diseño y por defecto;
    - realizar un registro de actividades de tratamiento;
    - establecer medidas de seguridad y realizar notificaciones de brechas de seguridad;
    - elaborar una evaluación de impacto en la protección de datos;
    - designar un delegado de protección de datos.

IV.C.3. Bases legales para el procesamiento de datos.

Las legislaciones suelen establecer un catálogo de bases legales que legitiman el tratamiento. En términos generales, el consentimiento de los interesados es la base legal más utilizada, al menos en la región. Al respecto, se suele requerir que los titulares de datos brinden su consentimiento libre, previo, expreso e informado para el procesamiento de su información personal.

Algunas leyes también proponen otras bases legales alternativas que legitiman las actividades de procesamiento de datos y que están destinadas a facilitar las operaciones comerciales de los responsables del tratamiento, como es la existencia de una relación contractual o precontractual con los interesados; la necesidad del responsable del tratamiento de cumplir con una obligación legal; la protección de los intereses vitales de los interesados o de terceros; la necesidad del responsable del tratamiento de realizar una tarea de interés público o de autoridad oficial, etc..

Especial atención merece el interés legítimo del responsable del tratamiento o de un tercero. Esta base legal podría ser utilizada en la medida que los intereses legítimos perseguidos no prevalezcan los intereses o los derechos y libertades fundamentales del titular que requiera la protección de datos personales, en particular cuando el titular sea niño, niña o adolescente[42].

Más allá del consentimiento, sería valioso que el tratado internacional prevea un catálogo razonablemente amplio de bases legales que legitimen el tratamiento susceptible de adaptarse a las numerosas circunstancias y casos que pueden plantearse. Eventualmente, podrían aceptarse supuestos adicionales como la ejecución de las políticas públicas previstas en las leyes o reglamentos, el ejercicio de derechos judiciales, administrativos o de arbitraje, la realización de estudios por parte de entidades de investigación y la protección del crédito, etc.

Por último, cabe mencionar el consentimiento para el tratamiento de los datos personales de los menores de edad. Los niños, niñas y adolescentes son considerados como un grupo vulnerable especialmente susceptible a las consecuencias del tratamiento de la información que les concierne, por lo que se requiere su protección integral y bienestar. Tanto en los casos de los Estándares Iberoamericanos como en el RGPD, el consentimiento de menores es sometido a la autorización de los titulares de la patria potestad, o quienes ejerzan su representación legal, quienes serán los responsables por las consecuencias del tratamiento[43]. Entiendo que esta es la posición que deberá prevalecer en el marco normativo internacional, permitiendo a cada Estado que establezca la edad mínima de los menores para que, por si mismos, puedan otorgar el consentimiento. Ello en tanto no existe una posición uniforme en cuanto a la edad a partir de la cual un menor puede prestar su consentimiento y sería muy difícil conseguir un consenso internacional al respecto.

IV.C.4. Obligación de transparencia.

[42] Art. 4.3.i) de los Estándares Iberoamericanos de Protección de Datos Personales.
[43] Informe de las Naciones Unidas preparado por la Relatora Especial sobre el derecho a la privacidad Ana Brian Nougreres, A/77/196: Principios que informan la privacidad y la protección de datos personales.

Al momento de la recopilación de datos, los responsables del tratamiento deben cumplir con la obligación de transparencia. El propósito de esta obligación es garantizar el derecho de los titulares de datos a recibir información concisa, clara, inteligible, detallada y fácilmente accesible sobre las condiciones del procesamiento de datos, por escrito o por otros medios. Si bien las normas basadas en el sistema europeo han reconocido su importancia, el deber de transparencia se encuentra previsto también en los textos legales norteamericanos, como es el caso de la Ley de Portabilidad y Responsabilidad de Seguros de Salud (*Health Insurance Portability and Accountability Act of 1996 - HIPAA*).

Habitualmente las leyes de protección de datos requieren que los responsables de tratamiento proporcionen la siguiente información a los titulares de datos: (i) la identidad y los detalles de contacto del responsable del tratamiento; (ii) los propósitos y la base legal del procesamiento de datos; (iii) el destinatario o las categorías de destinatarios de los datos personales, si los hubiera; (iv) la transferencia internacional de datos personales prevista y la naturaleza adecuada o inadecuada de las jurisdicciones a las que se transferirán los datos; (v) los derechos de protección de datos personales reconocidos a los titulares; (vi) los datos de contacto del delegado de protección de datos, de corresponder; (vii) el período de almacenamiento previsto o los criterios para determinar ese plazo; (viii) la voluntariedad u obligatoriedad en proporcionar datos personales y las consecuencias de brindar datos personales, de no hacerlo o de entregar datos personales inexactos; (ix) el derecho a presentar un reclamo ante las autoridades de protección de datos correspondiente; entre otra información relevante.

Aunque la lista de información obligatoria alcanzada por la obligación de transparencia puede diferir, las leyes locales tienden a incluir este principio. Con el objetivo de llegar a un acuerdo, un tratado internacional podría proponer la información obligatoria que no puede ser excluida por las regulaciones locales permitiendo a los países ampliar la lista a su voluntad. Entiendo que el catálogo de elementos enunciado arriba sería la información que debería considerarse esencial. Adicionalmente, el marco internacional deberá establecer que la información que se brinde al titular del dato sea proporcionada en lenguaje sencillo, claro, inteligible y de fácil acceso y comprensión, teniendo especial atención el nivel social y cultural del destinatario, particularmente en el caso de menores de edad.

IV.C.5. Derechos de los titulares de datos.

La mayoría de las leyes de protección de datos reconocen ciertos derechos a favor de los titulares. El abanico de derechos claramente no es el mismo en las distintas jurisdicciones pero considero que se podría lograr un consenso sobre la base de la aceptación de derechos básicos tales como los siguientes:

- Derecho de información: los titulares deben poder conocer de antemano las características y particularidades del tratamiento al cual serán sometidos sus datos personales.

- Derecho de acceso: los titulares de datos deben contar con el derecho a saber si el responsable del tratamiento está procesando información personal sobre ellos y obtener acceso a los mismos.

- Derecho de rectificación: los titulares de datos deben tener el derecho a obtener del responsable del tratamiento sin dilación indebida la rectificación de los datos personales inexactos que les conciernen.

- Derecho a la supresión: los titulares de datos deben tener derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan cuando concurran determinadas circunstancias. Al respecto, es importante señalar que algunas legislaciones han reconocido expresamente el derecho al olvido digital, como es el caso del RGPD.

  El derecho al olvido podría ser definido como la prerrogativa que posee toda persona para obtener la supresión de cierta información que, aun siendo correcta o referirse a hechos verídicos del pasado, ha perdido actualidad y, por ende, deja de ser pertinente a los efectos de su tratamiento salvo que en el caso concreto prevalezca un interés público en su mantenimiento. En ciertos supuestos se trata de información deshonrosa, denigrante, indecorosa, vergonzante que, puesta a disposición a través de las distintas herramientas tecnológicas que permiten la rápida y masiva difusión, puede dar lugar a afectaciones a la privacidad, honor,

honra, dignidad y/o reputación de la persona. En estos casos estamos en presencia de información que, como consecuencia del paso del tiempo, deviene innecesaria o impertinente para cumplir los fines para los cuales fue recolectada.

El propósito del derecho al olvido en Internet es limitar el acceso a cierta información obstaculizando legalmente la difusión y circulación. Por ende, si bien no se suprimen los datos, se restringe la posibilidad de poder llegar a ellos. Si determinado buscador deja de indexar el contenido cuestionado, la información seguirá existiendo, pero su acceso será más complejo para el usuario[44].

Si bien es cierto que sería sumamente valioso que el marco normativo internacional reconozca el derecho al olvido digital, teniendo en cuenta la relevancia que posee el derecho a la libertad de expresión para algunos sistemas jurídicos como es en el caso de los Estados Unidos, su incorporación podría ser conflictiva al punto tal de entorpecer las tratativas y negociaciones. Por ello, en un principio no se propondría su inclusión.

- Derecho a la limitación del tratamiento: el titular de los datos personales tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos en determinados casos. En efecto, en las siguientes situaciones podría reconocerse el derecho: (i) cuando se impugne la exactitud de los datos durante un plazo que permita al responsable verificar la exactitud de la información; (ii) cuando el tratamiento sea ilícito pero el titular en lugar de requerir la supresión de los datos personales solicite la limitación de su uso; o (iii) cuando el titular precise la información para ejercer una acción judicial y se oponga a que el responsable elimine esos registros, entre otros casos.

- Derecho a la portabilidad de datos: Si se tratan datos personales mediante medios electrónicos o automatizados, el tratado internacional debería reconocer al titular de los datos el derecho a la portabilidad. Conforme varias legislaciones que así lo prevén, debería garantizarse al titular el derecho a obtener una copia de la información que hubiese proporcionado al responsable del tratamiento o que sea

[44] Peruzzotti, Mariano. 2022 "El caso "Denegri": cuando la libertad de expresión prevalece sobre el derecho al olvido". *Diario La Ley*, 2022-D, Buenos Aires: Ed. Thomson Reuters La Ley. P. 7.

objeto de procesamiento en un formato que le permita su ulterior utilización por parte de otro responsable de tratamiento. El titular de los datos debe poder solicitar que sus datos personales se transfieran directamente de responsable a responsable si ello fuera técnicamente posible.

- Derecho de oposición: Las legislaciones suelen también reconocer el derecho del titular de los datos a oponerse en cualquier momento a que sus datos sean objeto de tratamiento, incluida la elaboración de perfiles así como para fines de marketing. El tratado internacional debería también incorporar esta potestad. Una vez ejercido el derecho, el responsable del tratamiento deberá dejar de tratar los datos personales a menos que demuestre motivos legítimos e imperiosos que justifiquen el tratamiento y que prevalezcan sobre los derechos de los titulares de los datos o, eventualmente, cuando sea necesario continuar con el procesamiento para el establecimiento, ejercicio o defensa de reclamos legales.

- Derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado: El tratado internacional deberá reconocer a los titulares de datos el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado que produzca efectos jurídicos en ellos o les afecte de forma similar de forma significativa, incluida la elaboración de perfiles.

- Derecho a presentar un reclamo ante las autoridades respectivas: Los titulares de datos deben tener reconocido el derecho a presentar un reclamo ante las autoridades competentes si consideran que el tratamiento infringe el marco internacional de protección de datos o las leyes nacionales respectivas. El titular de los datos debe poder optar por recurrir por la vía administrativa o judicial, dependiendo de las características y particularidades de cada sistema.

Los responsables de tratamiento deben asegurar a los titulares de los datos el ejercicio de sus derechos de forma gratuita y en el plazo establecido al respecto. En cuanto a este último punto, es cierto que no existe un consenso en las legislaciones locales sobre el término para responder los requerimientos de los titulares de los datos. En efecto, las empresas con actividades internacionales enfrentan serios inconvenientes al tratar de cumplir con regulaciones que imponen diferentes condiciones y plazos para responder.

Siendo ello así, la concesión de términos breves suele constituir un obstáculo que conspira contra la atención adecuada del pedido. En efecto, las empresas gestionan una gran cantidad de datos, lo que dificulta el procesamiento de las solicitudes de los titulares y la verificación de su identidad en plazos escuetos. La complejidad aumenta cuando los datos han sido transferidos a un encargado del tratamiento, ya que esto implica la participación de otro sujeto en la gestión de la petición.

A modo de ejemplo, el plazo otorgado por la legislación argentina (10 días corridos para la respuesta al derecho de acceso y 5 días hábiles para el caso de los derechos de rectificación, corrección, supresión y trato confidencial) ha sido siempre considerado demasiado breve. Por ende, la solución adoptada por el RGPD que concede un mes para responder parece ajustarse a las características actuales de los negocios. Inclusive, el otorgamiento de prórrogas para casos que requieran más tiempo para procesar el pedido es una opción que parece justa y razonable.

Adicionalmente, las leyes de protección de datos personales proporcionan ciertas excepciones en las cuales los responsables del tratamiento pueden negar a los titulares de datos el ejercicio de sus derechos como cuando el procesamiento es necesario por razones de interés público, entre otras. Este aspecto podría estar sujeto a lo que cada Estado resuelva considerando los marcos normativos locales. No obstante, las excepciones que se reconozcan a nivel local no podrán desarticular o afectar el espíritu del marco internacional, el cual tiene como uno de sus propósitos esenciales garantizar la autodeterminación informativa.

IV.C.6. Obligaciones de seguridad.

Según la mayoría de los estatutos, el responsable y el encargado de tratamiento deben implementar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de la información. El tratado internacional deberá incluir la obligación de seguridad como un principio clave para proteger los datos. No obstante, entendemos que el texto debe ser lo más amplio posible de modo tal de poder abarcar

todas las industrias y actividades de procesamiento. Es en base a ello que se sugiere recurrir a una propuesta que tienda a ser tecnológicamente neutral. La diversidad de las tecnologías, así como su transformación constante y dinámica, deben ser tomadas en cuenta al evaluar con responsabilidad, los riesgos y las medidas de seguridad adecuadas, por parte de las organizaciones.

Las medidas de seguridad deberán considerar el estado de la técnica, los costos de implementación y la naturaleza, alcance, contexto y propósitos del procesamiento, así como el riesgo de variabilidad y severidad para los derechos de los titulares de datos. En la práctica, cada actividad podrá escoger el catálogo de medidas que considere efectivas y que podrían incluir la pseudonimización, el cifrado de datos, los controles de acceso a sistemas físicos y virtuales, la gestión de pérdida de datos, las copias de seguridad, la realización de auditorías y testeos, entre otras medidas tendientes garantizar la confidencialidad, integridad, disponibilidad y resiliencia continua de los sistemas y servicios de procesamiento. Para ello podrá recurrirse a los estándares internacionales como las normas ISO o el marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés).

En este punto entiendo que las organizaciones son las indicadas para establecer cuál es el mecanismo de seguridad que mejor se adapta a sus prácticas y deben ser ellas las que definan el sistema a implementar considerando el tipo de procesamiento de datos que realicen, el negocio involucrado y otras circunstancias que rodean el flujo de datos. El tratado internacional solo debería sentar los principios y directrices generales.

Distintos documentos internacionales y nacionales incluyen la obligación de notificar los incidentes de seguridad a las autoridades de control y, en ciertos casos, a los titulares de datos afectados. En la lista de instrumentos que lo contemplan podemos mencionar al Convenio 108+[45], los Estándares, el RGPD, las Directrices, el Marco de Privacidad, la Ley General de Protección de Datos Personales de Brasil, las normas locales aprobadas en distintos Estados de los Estados Unidos, entre muchos otros. Un convenio internacional ayudaría a compatibilizar las exigencias regulatorias de las

[45] Protocolo modificatorio del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos con carácter personal, suscripto en la Ciudad de Estrasburgo, Francia, el 10 de octubre de 2018.

diferentes normas locales facilitando el reporte de las brechas de seguridad. El sistema de colaboración que se desarrolla más abajo podría establecer el canal de comunicación respectivo a la autoridad competente según determinados patrones o puntos de contacto.

IV.C.7. Evaluación de impacto en materia de protección de datos.

Las legislaciones nacionales suelen requerir la realización de una evaluación de impacto en materia de protección de datos personales cuando exista la posibilidad de que un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades del titular del dato. Estas evaluaciones permiten a las organizaciones identificar y tratar los riesgos que puedan producir sus actividades habituales y sus nuevos desarrollos que involucran el tratamiento de datos personales. Este es un punto que considero muy importante teniendo en cuenta la evolución de las tecnologías y comunicaciones, en especial la penetración de la Inteligencia Artificial en los distintos procesos y soluciones.

Siguiendo los estándares generales de las leyes de protección de datos más modernas, el tratado internacional podría prever la obligatoriedad de efectuar las evaluaciones en los siguientes supuestos:

a) en el caso de la evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles y, sobre cuya base, se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente;

b) en caso de realizar un tratamiento a gran escala de datos sensibles, o

c) en caso de la observación sistemática a gran escala de una zona de acceso público, videovigilancia o monitoreo regular y constante de conductas de las personas.

Las legislaciones suelen también indicar el contenido mínimo que debe incluir la evaluación y, en algunos casos, prevén la consulta previa a la autoridad local si el resultado de la evaluación revela un gran riesgo para los derechos de los titulares de datos.

El marco internacional podría establecer lineamientos generales y permitir que los respectivos Estados reglamenten las condiciones específicas al respecto.

IV.C.8. Confidencialidad y transmisión de datos personales.

Como regla general, los responsables y encargados de tratamiento deben guardar secreto en cuanto a los datos personales que recolectan y procesan. Una consecuencia de esa obligación de confidencialidad se refleja en la restricción a la transmisión de datos personales. Para poder compartir datos personales con terceros es preciso encontrar una base legal que valide esa divulgación. En ciertos casos las partes deben suscribir convenios específicos dependiendo si el destinatario de los datos actúa como responsable, co-responsable, encargado de tratamiento o subprocesador. El tratado internacional podría establecer las condiciones mínimas que validen las transmisiones así como los elementos que deban reunir los acuerdos cuando estos sean necesarios.

Como se ha analizado arriba, las leyes de protección de datos suelen restringir la transferencia internacional. Al respecto, el tratado podría prever exigencias adicionales para transferir datos a países que no han suscripto el documento. Claramente, ninguna condición adicional se requerirá para el caso de Estados que sean parte en base a que ellos garantizarán un mismo nivel de protección siendo que habrán adecuado previamente su legislación interna conforme el convenio.

Para el caso de países que no adhieran al convenio internacional, será preciso establecer requisitos para el flujo transfronterizo de manera tal que los datos se mantengan protegidos en el lugar de destino como lo estarían en cualquier Estado miembro del arreglo internacional. Para ello, se podría exigir la suscripción de contratos de transferencia internacional que sigan los estándares internacionales como las cláusulas contractuales adoptadas por distintos órganos supranacionales, a saber el Consejo de Europa, la Comisión Europea (Unión Europea), la Asociación de Naciones del Sudeste Asiático o la Red Iberoamericana de Protección de Datos. También se podría permitir que cada Estado parte elabore y apruebe cláusulas modelo para la transferencia internacional o sentar las bases para un nuevo sistema en el marco de la convención internacional que se propone.

Otras opciones para legitimar la transferencia podrían provenir de normas corporativas vinculantes (*Binding Corporate Rules*), mecanismos de certificación o códigos de conducta. También podría contemplarse situaciones de excepción en las que no apliquen las restricciones a la transferencia, tales como las siguientes:

a) cuando el titular del dato haya dado explícitamente su consentimiento a la transferencia propuesta;

b) cuando la transferencia sea necesaria para la ejecución de un contrato o medidas precontractuales;

c) cuando la transferencia sea necesaria por razones importantes de interés público;

d) cuando la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamos o acciones judiciales;

e) cuando la transferencia sea necesaria para proteger los intereses vitales del titular del dato o de otras personas; etc.

Cabe tener en cuenta que las disposiciones sobre transferencia internacional deberán ser redactadas de forma tal que permitan la libre circulación de datos, elemento que apuntala la economía digital y desempeña un papel fundamental en el crecimiento y la innovación. Por ende, el tratado internacional y las leyes locales no deberían fijar prohibiciones absolutas a la transferencia internacional de datos personales y, en cambio, proporcionar mecanismos que garanticen la seguridad de los datos transferidos siguiendo un estándar equivalente al del país de origen de los datos. Al mismo tiempo, no se deberían imponer requisitos de localización de datos para el sector público y/o privado, ya que ello no mejora la protección sino que, por el contrario, impide la innovación al limitar los servicios disponibles para las personas.

IV.C.9. Cooperación.

Cada Estado miembro debería designar una autoridad de control encargada de supervisar el cumplimiento de las disposiciones del convenio internacional dentro de sus

fronteras. En efecto, cada regulador local será competente para desempeñar las tareas que se le asignen en su propio territorio. Muchos países ya han creado sus respectivas autoridades y ellas podrían continuar actuando en el ejercicio de sus funciones.

Para poder conciliar los esfuerzos de supervisión, evitar conflictos jurisdiccionales y facilitar la colaboración internacional, se podría prever un mecanismo de cooperación que permita la resolución de controversias y reclamaciones así como llevar adelante las investigaciones y el control de las normas. Las autoridades nacionales deberían facilitarse recíprocamente información y prestarse asistencia mutua a fin de aplicar las disposiciones del convenio internacional de manera coherente y efectiva.

Cada Estado deberá tomar medidas para asegurar la efectiva cooperación entre reguladores. La asistencia mutua deberá comprender, en particular, las solicitudes de información y las medidas de control, como las solicitudes para llevar a cabo gestiones y ejecutar inspecciones e investigaciones.

También podría preverse un mecanismo de resolución de conflictos jurisdiccionales para los casos en los que un determinado tratamiento de datos pueda afectar dos o más territorios y sea necesario definir la autoridad principal que entenderá en el caso concreto. En este sentido, se podría delinear reglas que definan puntos de conexión para establecer la jurisdicción que tenga más cercanía con el caso, como podría ser el país de residencia de la mayor cantidad de titulares de datos comprometidos, el lugar en el que se encuentre el establecimiento principal del responsable o encargado, el sitio en el que se produjo el hecho, etc.

Una vez definida la autoridad principal que será competente, las demás oficinas estaduales deberían brindar asistencia en la investigación lo que implica intercambiar información, realizar operaciones conjuntas y simultáneas, colaborar en la ejecución y supervisión posterior de la decisión definitiva y/o participar en las medidas preventivas que se adopten, especialmente si las mismas tienen efectos en otro país.

Un procedimiento de cooperación similar podría estructurarse para la resolución de controversias judiciales. Ello permitiría que, con sustento en los principios de cortesía internacional y reciprocidad, una sentencia dictada por un tribunal competente en un

Estado parte sea reconocida para su ejecución por otro Estado parte. A su vez, este mecanismo garantizaría que los resortes que disponga el convenio internacional sean realmente eficaces.

IV.C.10. Comentarios finales sobre los elementos de la propuesta.

Los institutos mencionados precedentemente son los que, según mi entender, deberían conformar la estructura básica del sistema normativo supranacional en materia de protección de datos personales. Definitivamente, podrían incluirse otras figuras y elementos en la medida que se logre un consenso en cuanto a su incorporación.

No caben dudas que sería ideal que el instrumento sea lo más exhaustivo y completo posible. Sin embargo, y tal como hemos mencionado arriba, lograr la conformidad de múltiples sectores y Estados parece ser más asequible si se parte de la base de un documento genérico que incluya los aspectos esenciales en lugar de pretender ser rigurosamente detallista.

V. Desafíos que surgen al avanzar hacia la privacidad global.

La unificación normativa de la protección de datos personales implica desafíos y dificultades que no pueden ser ignorados. Uno de los grandes retos que deberá sortear el proyecto se deriva de las diferentes posiciones adoptadas por la Unión Europea y los Estados Unidos sobre la protección de los datos personales. El contexto actual demuestra que llegar a un acuerdo sobre el marco internacional no será tarea fácil.

Las distintas concepciones existentes sobre la protección de datos personales a nivel global traen desafíos adicionales a la hora de armonizar las normas. La variedad de guías, convenciones y otros instrumentos que se han promulgado a nivel internacional dificultan las posibilidades de llegar a un acuerdo sobre un marco internacional único[46]. En efecto, hay divergencias en cuanto al carácter vinculante o no vinculante que deberá adoptar el texto así como en lo que respecta al marco institucional o ad-hoc de su desarrollo, entre otros aspectos[47].

[46] KUNER. *Groningen Journal of International Law*, 2014, p. 58.
[47] KUNER. *Groningen Journal of International Law*, 2014, p. 59.

Por otro lado, también es cierto que el grado de evolución de la disciplina no ha sido uniforme en las distintas geografías. En efecto, la protección de datos no está plenamente desarrollada en algunos Estados. Mientras que en Europa se comienza a discutir la tercera generación de normas de protección de datos, en otras jurisdicciones aun no se ha sancionado siquiera el primer estatuto legal. Ello sugiere que un instrumento jurídico internacional vinculante que cubra la protección de datos podría ser prematuro.

Los mismos impedimentos para la adopción de un marco jurídico internacional que existían hace años siguen vigentes hoy en día, a saber, la falta de una organización internacional que supervise el trabajo, las diferencias culturales y jurídicas entre los sistemas de legislación y la incertidumbre sobre cómo podrían aplicarse tales normas a nivel nacional. Sin embargo, aunque las posibilidades a corto plazo de una amplia armonización sean reducidas, ello no debería ser un obstáculo para iniciar el diálogo y los trabajos tendientes a lograr un consenso que sirva de base para construir gradualmente un marco global. Todo ello es coherente con una visión pluralista y global de la protección de datos.

No se escapa a este análisis que la redacción de un convenio internacional probablemente demande años de discusiones. La experiencia indica que la celebración de un convenio multilateral para la armonización jurídica puede requerir largas tratativas que se extiendan en el tiempo, más aún cuando existen posiciones encontradas. Sin embargo, los beneficios generales que se obtendrían de conseguir dicha armonización constituyen incentivos suficientes para insistir en un marco supranacional.

La protección de datos personales merece brindar mayor seguridad jurídica a cada sujeto involucrado y, al mismo tiempo, una mayor tutela a escala mundial. Ha llegado el momento de adoptar un enfoque global de la protección de datos. Dicho ello, merece señalarse también que los esfuerzos de armonización jurídica mundial deben ser lo suficientemente flexibles como para abarcar enfoques que vayan más allá de los instrumentos tradicionales[48].

[48] KUNER. *Computer Law & Security Review*, 2009, p. 29.

Sería beneficioso para el desarrollo del marco global que la comunidad internacional dedicara mayores esfuerzos tendientes a relevar las áreas de convergencia en los distintos ordenamientos jurídicos. Una mayor comprensión mutua de los enfoques culturales y jurídicos de la protección de datos en el mundo ayudaría a crear las condiciones para la eventual adopción de un marco internacional.

Es menester continuar avanzando hacia un equilibrio entre los distintos intereses involucrados en el tratamiento de datos personales en la era global y digital en la que nos encontramos, en pos de la cooperación y la armonización normativa. Ese debería ser el norte a seguir.

VI. Conclusiones.

La protección de datos personales ha adquirido un aspecto transnacional indudable. Mientras que no hace mucho tiempo, el responsable del tratamiento, el titular de los datos y los medios utilizados para el procesamiento de datos estaban situados generalmente en un mismo país, el desarrollo del comercio internacional, las nuevas tecnologías y las modernas estructuras corporativas multinacionales han modificado ese paradigma. Hoy los datos personales no conocen de fronteras.

Este nuevo entorno ha puesto en crisis la noción territorial de las leyes de protección de datos. Es así como la respuesta a esta problemática ha sido extender extraterritorialmente el alcance de las disposiciones de los cuerpos normativos locales. Ello ha representado un grave trastorno para organizaciones que se nutren de actividades de tratamiento de datos en múltiples jurisdicciones, como se ha desarrollado a lo largo del presente trabajo. La actual falta de claridad en el contexto de la privacidad global crea incertidumbre para los titulares de datos, las empresas y las autoridades, al mismo tiempo que restringe el alcance del intercambio transfronterizo y sofoca el crecimiento económico y social[49].

Los nuevos desarrollos tecnológicos están sumando un argumento adicional a la necesidad de un marco legal de protección de datos personales internacional, sólido,

[49] KUDOS, Nicky, *Privacy Legislation Goes Global (Slowly!) Are You Prepared?*, 2019.

integral y consistente. A medida que la economía interrelacionada avanza hacia un espacio virtual conectado, la necesidad de abordar las preocupaciones de privacidad de forma global seguirá en aumento.

Hemos visto que se ha producido un fenómeno peculiar: mientras la internacionalización de las actividades de procesamiento de datos ha crecido exponencialmente en los últimos años, al mismo tiempo todas las iniciativas regulatorias han sido locales o, a lo sumo, regionales. Se ha pretendido regular localmente actividades con claros rasgos internacionales. Por lo tanto, los esfuerzos tendientes a armonizar la legislación sobre privacidad en todo el mundo requieren atención urgente. La globalización de la sociedad y la omnipresencia de las comunicaciones electrónicas hacen imperativo que el derecho a la protección de datos sea aplicable y exigible a nivel internacional[50].

Un régimen internacional de protección de datos no solo es deseable para promover la inversión sino también para proporcionar una salvaguardia legal en la materia que sea uniforme en todo el mundo. Esto incrementaría la confianza de los titulares de datos y simplificaría la cooperación mutua entre las autoridades locales permitiendo un control más efectivo y eficiente. La construcción de puentes entre los diferentes sistemas de protección de datos resulta esencial para facilitar el crecimiento económico y al mismo tiempo dotar de recursos novedosos que generen un entorno de mayor protección a la privacidad a nivel supranacional.

Ciertamente, las dificultades políticas que puede conllevar la armonización global de la privacidad demuestran que la negociación de un marco legal internacional no será un camino de rosas. Se necesitará un entendimiento mutuo sobre las diferentes tradiciones culturales y legales a fin de crear las condiciones adecuadas para la eventual adopción de un marco global.[51] Sin embargo, los problemas actuales que atraviesa la disciplina exigen un gran esfuerzo para lograr un marco legal internacional. Definitivamente, guardar silencio sobre este tema en el contexto de una economía cada vez más globalizada donde

[50] KITTICHAISAREE. KUNER, *European Journal of International Law*, 2019.
[51] KUNER. *Groningen Journal of International Law*, 2014, p. 67.

cada día se realizan más actividades económicas en línea no es una opción viable y válida.[52]

Por lo tanto, aún reconociendo los retos que implica lograr los consenso necesarios para acordar un tratado internacional, considero que la armonización de las legislaciones de protección de datos sin duda aportaría beneficios sustanciales para toda la comunidad. Este trabajo ha intentado dar cuenta de ello, planteando los problemas que atraviesa la disciplina y proponiendo los elementos que pueden servir de base a un posible marco regulatorio global.

[52] UNITED NATIONS, *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, 2016. Disponible en el siguiente sitio: https://www.tralac.org/images/docs/9500/data-protection-regulations-and-international-data-flows-implications-for-trade-and-development-unctad-april-2016.pdf (última consulta: 30 de septiembre de 2023).

Bibliografía

1. Alo, Edward. "EU Privacy Protection: A Step Towards Global Privacy", *Michigan State International Law Review*, Vol. 22.3, 2014, (https://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?article=1155&context=ilr; (última consulta: 30 de septiembre de 2023).
2. Azzi, Adèle. "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation", *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 9 (2), 2018. (https://www.jipitec.eu/issues/jipitec-9-2-2018/4723; última consulta: 30 de septiembre de 2023).
3. Basterra, M. I. *Protección de datos personales: ley 25.326 y dto. 1558/01 comentados; derecho constitucional provincial, Iberoamérica y México*. 2008. Buenos Aires: EDIAR.
4. Bougiakiotis, Emmanouil. "The Layered Links Model: An Alternative Approach to International Privacy Regulation", *International Data Privacy Law*, Vol. 10, Issue 3, 2020, (https://ssrn.com/abstract=3464380; última consulta: 30 de septiembre de 2023).
5. Determan, Lothar. *Protección Global de Datos Personales*. 2020. Buenos Aires: Astrea.
6. Faliero, Johanna. *La protección de datos personales*. 2021. Buenos Aires: AdHoc.
7. Kittichaisaree, Kriangsak; Kuner, Christopher. "The Growing importance of Data Protection in Public International Law". *European Journal of International Law*. Vol. 30, Nr. 3. August 2019.
8. Kuner, Christopher. "An International Legal Framework for Data Protection: Issues and Prospects*", Computer Law & Security Review*, Vol. 25, 2009, pp. 307-317, (https://ssrn.com/abstract=1443802; última consulta: 30 de septiembre de 2023).
9. Kuner, Christopher. "Data Protection Law and International Jurisdiction on the Internet (Part 1)". *International Journal of Law and Information Technology*, Vol. 18 No. 2, Oxford University Press, 2010. (https://doi.org/10.1093/ijlit/eaq002; última consulta: 20 de septiembre de 2023).

10. Kuner, Christopher. “Data Protection Law and International Jurisdiction on the Internet (Part 2)”. *International Journal of Law and Information Technology*, Vol. 18 No. 3, Oxford University Press, 2010. (https://academic.oup.com/ijlit/article-abstract/18/3/227/836305; última consulta: 20 de septiembre de 2023).
11. Kuner, Christopher. “The European Union and the Search for an International Data Protection Framework”, Groningen Journal of International Law, Vol. 2, Ed. 1: Privacy in International Law, 2014. (http://www.kuner.com/my-publications-and-writing/untitled/kuner-groningen-journal-von.pdf; última consulta: 20 de septiembre de 2023).
12. Kuner, Christopher, “Extraterritoriality and International Data Transfers in EU Data Protection Law”. *International Data Privacy Law,* Vol. 5, Issue 4, 2015 (https://academic.oup.com/idpl/article-abstract/5/4/235/2404454?campaignid=20594288625&adgroupid=&adid=&gclid=CjwKCAjw9-6oBhBaEiwAHv1QvBcufs22fGotsxjiZN2k-KX_6fh3Q6AHZItEbZnqmAQm4VV-slR9ihoCc8AQAvD_BwE; última consulta 30 de septiembre de 2023).
13. *Groningen Journal of International Law,* Vol. 2, Ed. 1: Privacy in International Law, 2014 (http://www.kuner.com/my-publications-and-writing/untitled/kuner-groningen-journal-von.pdf; última consulta: 30 de septiembre de 2023).
14. Kudos, Nicky. “EU Versus US Privacy Legislation – Convergence?” Disponible en sitio: https://www.kudos-data.com/eu-versus-us-privacy-legislation/; (última consulta: 30 de septiembre de 2023).
15. Palazzi, Pablo (compilador). *Protección de datos personales. Doctrina y jurisprudencia, Tomo 1*. 2021. Buenos Aires: CDYT. Colección derecho y tecnología.
16. Palazzi, Pablo (compilador). *Protección de datos personales. Doctrina y jurisprudencia, Tomo 2.* 2021. Buenos Aires: CDYT. Colección derecho y tecnología.
17. Palazzi, Pablo (compilador). *Protección de datos personales. Doctrina y jurisprudencia, Tomo 3*. 2023. Buenos Aires: CDYT. Colección derecho y tecnología.

18. Peruzzotti, Mariano. *Alcance territorial de las Leyes de Protección de Datos Personales.* Diario *La Ley*, Volumen 2020-F, 428. Buenos Aires: Thomson Reuters La Ley.

19. Peruzzotti, Mariano. *El caso Schrems II y sus implicancias en la región*. The Privacy Advisor. 2020. https://iapp.org/news/a/el-caso-schrems-ii-y-sus-implicancias-en-la-region/ (última consulta: 10 de abril de 2023).

20. Peruzzotti, Mariano. "Pasado, presente y futuro de la transferencia internacional de datos" en Palazzi, Pablo (compilador). *Protección de datos personales. Doctrina y jurisprudencia, Tomo 2.* 2021. Buenos Aires: CDYT. Colección derecho y tecnología.

21. Peruzzotti, Mariano. *El caso "Denegri": cuando la libertad de expresión prevalece sobre el derecho al olvido*. Diario La Ley, 2022-D, Buenos Aires: Thomson Reuters La Ley.

22. Puccinelli, Oscar R. *Protección de datos de carácter personal: comentario exegético de la ley 25.326 y su reglamentación*. 2004. Buenos Aires: Astrea.

23. Svantesson, Jerker. "Extraterritoriality in the context of data privacy regulation". *Masaryk University Journal of Law and Technology*, 2013. Vol 7, No. 1. (https://journals.muni.cz/mujlt/article/view/2628; última consulta: 30 de septiembre de 2023).

24. Svantesson, Jerker. "Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation". *International Data Privacy Law*, 2015. Vol 5, No. 4.

25. Taylor, Mistale. "The EU's human rights obligations in relation to its data protection laws with extraterritorial effect." *International Data Privacy Law,* 2015. Vol. 5, No. 4, p. 246, (https://academic.oup.com/idpl/article/5/4/246/2404460; última consulta: 30 de septiembre de 2023).

26. Travieso, Juan Antonio. *Régimen jurídico de los datos personales*. 2014. Buenos Aires: Abeledo Perrot – La Ley.

27. Ustaran, Eduardo. "European Data Protection. Law and Practice". 2018. Portsmouth, Estados Unidos: International Association of Privacy Professionals.

28. Vaninetti, Hugo Alfredo. *Derecho a la intimidad en la era digital, Tomo 1.* 2021. Buenos Aires: Hammurabi.

29. Vaninetti, Hugo Alfredo. *Derecho a la intimidad en la era digital, Tomo 2.* 2021. Buenos Aires: Hammurabi. Buenos Aires, 2021.

30. Warren, Samuel. Brandeis, Louis. *The right to privacy*. 1890. Estados Unidos de Norteamérica: Harvard Law Review, Vol. 4, No. 5, pp. 193-220.