IMPLICANCIAS ECONÓMICAS DE LA REGULACIÓN QUE BUSCA PROTEGER LOS DATOS PERSONALES EN CHILE

TESIS PARA OPTAR AL GRADO DE
MAGÍSTER EN POLÍTICAS PÚBLICAS

Alumno: Yael Schnitzer Raab
Profesor Guía: Óscar Landerretche Moreno

Santiago, diciembre de 2020

Tabla de Contenidos

Introducción

El aumento explosivo de información disponible, impulsado por el desarrollo tecnológico, aceleró la digitalización del mundo físico y provocó la llamada cuarta revolución industrial, que tiene como principal activo la información. Este nuevo escenario, cambió la forma en que percibimos la economía tradicional y la creación de valor, además de la estructura y la organización de los negocios, provocando el surgimiento de un nuevo concepto: la economía digital.

Este término fue acuñado por primera vez en 1994 por Don Tapscott, quien la describió como una economía basada en el conocimiento y que se alimenta de los datos que surgen de la virtualización de las actividades sociales y económicas. Donde la capacidad inmediata de recolectar, almacenar, procesar y compartir datos a gran escala, y a nivel global, permite maximizar el valor de la información en ambos lados del mercado (Tapscott, 1994).

El valor de la información es maximizado cuando: a) permite generar nuevos datos e información para mejorar o crear nuevos productos y servicios, más alineados a lo que el cliente desea; b) potencia el nacimiento de nuevos modelos, estructuras y organizaciones de negocio, que aumentan la eficiencia y reducen los costos; c) facilita la globalización de las empresas, sin importar su tamaño; y d) ayuda a reducir la asimetría de información entre consumidores y productores, al transparentar información respecto a la calidad de bienes y servicios.

El uso de grandes bases de datos (*big data*[1]), y de tecnologías que permiten la automatización de los procesos que requieren aprendizaje, como el *machine learning* y la

[1] Francis y Francis (2017, p.37) define *big data*, como grandes sets de datos recolectados por diversas entidades, y que se caracteriza por su volumen, varierad y velocidad.

Inteligencia Artificial (IA), no solo aumenta la eficiencia y eficacia de la maximización del valor de la información, sino que también puede generar ventajas competitivas derivadas del "efecto red de datos". Google es un clásico ejemplo de este efecto, puesto que mientras más personas utilizan el buscador, más datos proveen, permitiéndole a Google refinar y mejorar constantemente sus resultados de búsqueda y personalizar la experiencia del usuario, lo que a su vez aumenta el número de usuarios y los datos que entregan (Turck, 2016).

El efecto red de datos entrega ventajas competitivas tan relevantes, que puede generar la dinámica del "ganador se lleva todo" y amenazar el nivel de competencia de los mercados, porque el primero en acceder al *big data* que alimenta un nuevo negocio, obtiene todos los beneficios y concentra el mercado. Es lo que sucedió con Apple, Google, Microsoft, Amazon y Facebook, las cinco empresas más valiosas del mundo y que basan su modelo de negocio en el tratamiento masivo de datos (The Economist, 2017b). Estas empresas estadounidenses fueron pioneras, lograron obtener una posición dominante en el mercado global, gracias al acceso único, y uso exclusivo, de miles de millones de datos personales aportados por sus usuarios a lo largo de los años en diferentes lugares del mundo.

La información es considerada por los economistas como un "bien público", puesto que beneficia a todos incluso a aquellos que no han pagado acceder a ella (Francis y Francis, 2017). Sin embargo, existen cuatro grandes razones para que los datos personales sean objeto de protección. La primera es que la información personal hoy es monetizada por diferentes actores del mundo público y privado. La segunda, es que los datos personales son un bien no rival, por lo que pueden ser copiados y utilizados

simultáneamente por más de una persona (o algoritmo), y con un propósito distinto para el que fueron recolectados. La tercera, es que el uso de los datos personales tiene el potencial de generar beneficios o daños al titular de dichos datos. La cuarta, es que la economía guiada por los datos es imperfecta, presentando alto niveles de opacidad, grandes asimetrías de información y una fuerte tendencia a la concentración.

Los bancos utilizan la información para predecir el riesgo crediticio de una persona, las clínicas y hospitales buscan conocer factores de riesgo para ciertas enfermedades, y los buscadores y las redes sociales predicen qué publicidad es más adecuada para cada usuario, entre otras. El tratamiento de la información personal puede beneficiar a los consumidores, pero también puede afectarlos negativamente. Las personas pueden ser objeto de discriminación y ver limitada su autonomía (Francis y Francis, 2017). Conocer los factores de riesgo de una enfermedad nos beneficia a todos, pero deja de ser beneficioso, por ejemplo, si esa información se utiliza para denegar el acceso a un seguro de salud a cierta persona o es utilizada por otros ciudadanos para discriminar a una persona. Una empresa puede usar los datos personales de sus trabajadores o postulantes para decidir quién sale o ingresa de la compañía, mientras que los bancos pueden denegar créditos si la información que tenían en su poder predice un alto riesgo crediticio (Sampath, 2019).

La economía guiada por los datos presenta alto niveles de opacidad. Nadie sabe realmente qué hacen las compañías con los datos personales de sus usuarios y el conocimiento público de diversas brechas de seguridad, que afectaron la privacidad de miles de usuarios, ha aumentado de la sensación de riesgo y amenaza de un uso malicioso de los datos personales, han acrecentado la demanda ciudadana por mayor protección y control sobre sus datos personales.

Las regulaciones de protección de datos personales apuntan a limitar su uso y devolver el control de los datos a sus titulares, desde la perspectiva de derechos humanos que adopta la Unión Europea, y al mismo tiempo, busca proteger e incentivar la innovación que resulte de su tratamiento, desde una perspectiva económica o utilitaria. Las regulaciones que protegen los datos personales generan efectos económicos positivos y negativos, los cuales hay que conocer antes de optar por uno u otro modelo.

En este escenario, Aaronson y Leblond (2018) señalan la existencia de tres grandes reinos de datos en la actualidad: EEUU, China y la Unión Europea. Estos reinos, han logrado establecer una posición dominante y hoy luchan por fijar las reglas del juego del comercio digital, buscando regular el flujo transfronterizo de datos personales y la protección de los derechos de los titulares, de la forma que les resulte más conveniente desde una perspectiva económica.

A nivel internacional, los países están actualizando sus regulaciones en la materia y muchos de ellos han optado por el modelo europeo, que se ha consolidado como el modelo con los más altos estándares de protección. Las organizaciones internacionales, como la Organización para la Cooperación y el Desarrollo Económico (OCDE) y el Foro de Cooperación Económica Asia-Pacífico (APEC, por sus siglas en ingles), han publicado guías y lineamientos de protección de datos personales, buscando proteger los derechos de los titulares y más importante aún, desde su perspectiva, asegurar el libre flujo transfronterizo de datos, estableciendo reglas comunes o armonizando las diferentes regulaciones a nivel mundial.

Chile está tramitando un proyecto de ley que actualiza su regulación de protección de datos personales, que data de 1999, y que sigue los lineamientos de la Unión Europea, cumpliendo también con algunas directrices de la OCDE y la APEC. El alcance

extraterritorial del Reglamento General de Protección de Datos (RGPD), que ha consolidado su influencia a nivel global, y la necesidad de ser considerado "país adecuado", para poder realizar transferencias internacionales de datos relativos a ciudadanos europeos, fueron determinantes para optar por este modelo que ha sido imitado por muchos países en el mundo.

En este contexto, es importante evidenciar cuáles son las posibles implicancias económicas de una regulación de datos personales, basada en el modelo europeo, para Chile. Esta será la pregunta de investigación que guiará este trabajo, que comenzará por establecer en el primer capítulo cuál es el rol de los datos personales en la economía, cómo se genera valor y cuáles son los posibles costos y beneficios de ello. En el segundo capítulo abordaremos la regulación en materia de protección de datos de la Unión Europea (UE), su evolución e implicancias económicas. En el tercer capítulo expondremos la protección de datos personales a nivel mundial, las principales iniciativas internacionales de armonización, lideradas por la OCDE y la APEC, y la existencia de tres grandes reinos de datos, correspondientes a China, Estados Unidos (EEUU) y la UE. Finalmente, en el cuarto capítulo se analizará el caso de Chile. El estado actual de la legislación y del desarrollo de la economía digital, las principales características del proyecto de ley y sus posibles implicancias económicas.

Capítulo 1

El rol de los Datos Personales en la economía

Datos personales

Los datos son hechos o detalles no procesados, mientras que la información es un subconjunto de datos que han sido procesados, organizados o estructurados (Aaronson, 2018). Un dato personal es "toda información relativa a una persona natural identificada o identificable" (Artículo 4, RGPD).

Históricamente, el comercio ha utilizado distintas técnicas para obtener datos personales de sus clientes y convertirlos en información de valor para su negocio. Los comerciantes han utilizado los datos como un insumo para mejorar la calidad, la eficiencia y el precio de sus productos y servicios (Aaronson y Leblond, 2018). Una de las formas más tradicionales de recolectar datos, es solicitarlos directamente a su titular mediante una encuesta. Sin embargo, recolectar y analizar datos manualmente es un proceso lento y costoso, además de estar expuesto a errores humanos.

El desarrollo tecnológico cambió radicalmente la capacidad de generar, extraer y maximizar el valor de los datos. Hoy es posible recolectar, almacenar, procesar y transferir grandes bases de datos en tiempo real y de forma automatizada. Estamos experimentando una nueva economía basada en el conocimiento, la economía digital, donde se produce una virtualización de actividades sociales y económicas (Tapscott, 1994). Esta virtualización, ha generado un aumento explosivo de información disponible.

Reinsel, Gantz y Rydning (2018), afirman que la esfera de datos en el mundo crecerá de los 33 zetabytes en 2018 a 175 zetabytes en 2025. Esta esfera, se alimenta de los datos creados en: el núcleo (centros de datos tradicionales y en la nube), el borde (infraestructura reforzada por la empresa, como las torres de celulares o pequeños centros de datos) y el punto final (computadores, teléfonos inteligentes y dispositivos del Internet

de las Cosas). Incluso, los autores afirman que debido a la introducción de los datos en nuestro trabajo y diario vivir, casi el 30% de la esfera global de datos en 2025 corresponderá a información en tiempo real, proveniente del "borde" y el "punto final" (Reinsel et al, 2018).

El rol de los datos en el comercio cambió. "Hoy los individuos, las empresas y los gobiernos, utilizan los datos para crear nuevos sectores y servicios entregados a través de internet (…) Al hacerlo, están creando una nueva economía que se construye sobre la base de la transferencia transfronteriza de datos" (Aaronson y Leblond, 2018, p.1).

El comercio digital se sustenta en el flujo de datos a nivel mundial, y comprende todas las transacciones comerciales transfronterizas que son solicitadas, facilitadas o entregadas digitalmente (López y Jouanjean, 2017). De esta forma, abarca las transacciones del *e-commerce* (solicitado digitalmente), las tecnologías de la información y las comunicaciones (TICs) (entregadas digitalmente), y las plataformas digitales (que facilitan digitalmente transacciones). Es importante destacar que "no todos los flujos transfronterizos de datos resultan necesariamente en una transacción monetaria per se, pero sí podrían impulsar una, como aquella generada por las ganancias asociadas a la venta de publicidad" (OCDE, 2017, p.13). Facebook es un buen ejemplo de ello, es una red social que ofrece un servicio a cambio de datos personales, los que utiliza para generar ganancias en publicidad.

Existen tres formas de obtener datos personales en la economía digital. Los datos que provee voluntariamente una persona, los datos que se pueden observar y los datos que se pueden inferir. Cuando entregamos nuestro número de tarjeta de crédito, nombre y dirección personal, para poder realizar una compra online, estamos cediendo nuestra información conscientemente (entrega voluntaria de datos). Cada vez que una persona accede a una página web o plataforma digital deja un rastro, una huella digital, y las

empresas utilizan herramientas como las *cookies*[2] y los *spywere* (programa espía que recopila información y la transmite sin el conocimiento del usuario), para extraer información de la navegación de esa persona (datos observados). Estas dos fuentes de datos, se utilizan para crear nuevos datos, como hábitos de consumo, intereses y preferencias, sin que el individuo sea realmente consciente de ello (datos inferidos).

Entrega Voluntaria de Datos	**Datos observados**	**Datos inferidos**
Fotos, Blogs, mails, tweets, transacciones online, formularios de registros, postulación a trabajos.	Preferencias de navegación en la web, video vigilancia, datos de localización, registros de llamadas.	Puntaje de crédito, perfil del consumidor, predicción del flujo de tráfico, marketing dirigido.
World Economic Forum (2018, p12).		

Otra forma de categorizar los datos personales, es la que realiza Sampath (2019), quien establece una división entre los datos estructurados –aquellos generados por máquinas, como las aplicaciones del Internet de las Cosas[3] (IoT, por sus siglas en inglés), y que pueden acumularse para crear *big data*- y los datos desestructurados –creados a través del uso e interacción de las personas en internet.

[2] Las *cookies* son pequeños pedazos de código instalados en el computador que permiten a los sitios web reconocer al usuario cada vez que los visita. Existen tres tipos, el primero funciona en una misma sesión, el segundo en la página web visitada (buscando "mejorar la experienia del usuario") y la tercera, permite el seguimiento del usuario más allá de la página que visita (Francis y Francis, 2017).

[3] Francis y Francis (2017, p. 220), defien el internet de las cosas como la capacidad de los objetos de comunicarse entre sí a través del Internet.

El origen del dato es importante, puesto que determina la dinámica relacional en términos de la percepción de propiedad y control sobre éstos. Para las empresas, mientras más energía y recursos económicos se invierten en la generación de datos, mayor es la sensación de propiedad y control sobre éstos. Para los consumidores, mientras menos conscientes fueron de la creación de los datos (y más íntimos y predictivos se tornan), más aumenta su sensación de intrusión y de pérdida de control sobre estos (World Economic Forum, 2018).

Características del Mercado de los Datos Personales

La privacidad posee dos mercados: el de los datos personales y el de la privacidad. En el mercado de los datos personales, participan compañías que buscan saber más de sus clientes, empresas que trabajan con datos y personas dispuestas a vender, o ceder, su información. En el mercado de la privacidad, se tranzan productos y/o servicios que buscan garantizar o asegurar la protección de los datos personales y la seguridad de la información de personas y/o compañías. Esta investigación, pone su foco en el mercado de los datos personales. La economía digital necesita de ambos mercados, el de los datos personales y el de la privacidad, para desarrollar todo su potencial. Por un lado, su crecimiento depende de la capacidad de innovación de las compañías –que está fuertemente relacionada con la capacidad de recolección, procesamiento y transmisión de datos- y por el otro, su subsistencia depende de la confianza de los actores en el sistema.

Como bien expuso la APEC (2015):

> "La confianza de los consumidores en la privacidad y seguridad de sus transacciones online, redes de información y manejo de datos personales, es crítica para permitir a las economías miembros obtener los beneficios del comercio electrónico y participar en la actual economía basada en la información" (p.4).

Las plataformas digitales, al disponer información transparente sobre las mejores alternativas de productos y servicios, reducen el costo de oportunidad de consumidores y proveedores. Disminuyen la asimetría de información[4], sobre todo con respecto a la calidad de un bien o servicio, y al contar con sistemas de retroalimentación del consumidor y productor, fortalecen la confianza en ellas. "Esto ha permitido que personas desconocidas de polos opuestos del mundo, y que con certeza no tendrán otra transacción en el futuro, confíen e intercambien activos (tangibles y no tangibles) a través de las plataformas", (Comisión Nacional de Productividad, 2018, p.5).

Paralelamente, el perfeccionamiento del proceso de integración y encuentro entre los agentes en la economía digital, ha permitido a las plataformas digitales cobrar una tarifa óptima a cada usuario. La sensibilidad a la tarifa se vuelve más inelástica y esto ha permitido que "la parte más interesada en el servicio pueda subvencionar parcial o completamente a la otra" (Comisión Nacional de Productividad, 2018, p. 7). Esto ha impulsado el surgimiento de empresas digitales gratuitas como Google, Facebook y Twitter, que ofrecen sus servicios sin un costo directo a sus usuarios, sino que lo hacen a cambio de sus datos personales. Una base de datos amplia, o *big data*, les permite segmentar a los usuarios y alinear la publicidad a sus intereses. Esto beneficia a quien recopila y analiza los datos para vender espacios de publicidad dirigida a un grupo específico (como Google, motor de búsqueda); a quienes reciben dicha publicidad (potenciales consumidores que reciben información de su interés); y a quienes compran

[4] La asimetría de información se produce cuando uno de los participantes en un intercambio posee más información que los otros y por ende, surge el riesgo de selección adversa y el riesgo moral. Si la percepción de riesgo es muy alta, puede inhibir el intercambio y la existencia del mercado se ve amenazada. "La selección adversa se da cuando una parte no puede distinguir, previo al intercambio, un atributo relevante de la otra, porque dicho atributo no es observable (ej. Calidad de un auto usado) (…) El riesgo moral está presente cuando algunos de los atributos sobre los que se realizó la transacción se modifican luego de la misma" (comportamiento del asegurado, luego de contratar un seguro) (Comisión Nacional de Productividad, 2018, p. 4).

el espacio para publicitarse (empresas que apuestan por una inversión más eficiente y eficaz).

Sin embargo, "la nueva economía mediada por la tecnología es imperfecta, plagada de asimetrías de información, monopolios, opacidad algorítmica y efectos del 'ganador de lleva todo'", Sampath (2019). Las empresas utilizan la capacidad inmediata de recolectar, procesar y compartir datos a gran escala, y a nivel global, para generar nuevos datos e información certera, que ayudan a mejorar y/o crear nuevos productos, servicios y modelos de negocio. Mientras más datos posee una empresa, mayor es la capacidad de maximizar su valor. Existe una "externalidad positiva asociada al tamaño de la red, que a mayor número de 'usuarios oferentes' y 'usuarios demandantes' más eficiente hace a los algoritmos, más rápido crea la reputación, y mayores transacciones surgen" (Comisión Nacional de Productividad. 2018. p. 7). Esto se conoce como el efecto red de datos (*data network effect*) y su principal consecuencia es la concentración de los mercados.

Las grandes plataformas online se vuelven cada vez más dominantes, en parte, gracias a su habilidad para recolectar, almacenar y procesar los datos personales de sus usuarios. Es un mercado donde "el ganador se lleva todo" y, por ende, el valor y el potencial económico de los datos, queda restringido a los principales jugadores (Budzyn, 2019). En 2017, Amazon capturó la mitad de todos los dólares que se gastaron online en EEUU, y Google y Facebook, fueron responsables de casi el total del crecimiento del gasto en publicidad digital (The Economist, 2017b).

La *European Data Protection Board* [EDPB] (2018), declaró que "el aumento de la concentración en los mercados digitales, tiene el potencial de amenazar el nivel de protección de datos y la libertad de los consumidores de servicios digitales. La protección

de datos y los intereses de privacidad de los individuos son relevantes, para cualquier evaluación de potencial abuso de posición dominante y también las fusiones de compañías, que puedan acumular o ya acumulan un poder significativo de información".

Como podemos observar, "las plataformas dominantes pueden obtener ganancias si tienen un acceso único a datos personales o una habilidad única para seguir a los usuarios a través de los sitios web" (Athey, 2014, p. 9). Por ende, explica la autora, las empresas tienen el incentivo de diseñar políticas de privacidad que favorezcan esa posición dominante, lo que justificaría el desarrollo de nuevos marcos legales que garanticen la competencia en la economía.

En este escenario, surgen muchas transacciones donde "el individuo no tiene la capacidad de negociar un nivel deseado de protección de información; más bien enfrenta una oferta de servicio tómalo-o-déjalo a cambio de datos personales" (Acquisti, 2010, p.39). Para el autor, esto significa una clara asimetría de poder que favorece a las empresas sobre las personas. Por ejemplo, cuando una empresa alcanza una posición dominante en el mercado, como Facebook en la oferta de redes sociales, se produce una asimetría de poder entre consumidores y productores, puesto que, si un individuo quiere desarrollar su vida social en esa plataforma, deberá aceptar las políticas de privacidad que le ofrecen y su libertad de elección real se ve coartada (puesto que no tiene otra alternativa o capacidad de negociación).

Frente a las políticas de privacidad, los consumidores no solo se deben enfrentar a la asimetría de poder, sino que también a la asimetría de información. Como expuso, Motiwalla, Li, y Liu, (2014) "intentar comprender el flujo complejo e inescrutable de datos de las plataformas digitales es cada vez menos práctico. Es difícil medir el valor y las consecuencias de los diferentes usos de los datos a través de la cadena de valor". Esto

significa que es muy difícil comprender y comparar las diferentes políticas de privacidad entre una compañía y otra, por ende, segmentar la demanda para ofrecer niveles óptimos de privacidad no es fácil.

La privacidad es un derecho humano fundamental, contenido en el artículo 8 de la Declaración Universal de Derechos Humanos que señala: "Todos tienen el derecho a que se respete su vida privada y familiar, su casa y correspondencia" (Asamblea General de la Organización de las Naciones Unidas, 1948). En sus orígenes, este derecho tenía una expresión de tutela negativa, el derecho a ser dejado solo, y con el tiempo, evolucionó hacia una expresión de tutela dinámica, el derecho a la autodeterminación informativa, el cual permite a las personas decidir cómo se quieren presentar ante el mundo y, por ende, estar libres de interferencias e intrusiones no deseadas.

El World Economic Forum (2018, p.11), plantea que la protección de datos personales busca evitar que una "información sea incorrectamente asociada con una persona o que datos inexactos/incorrectos/imprecisos sean utilizados para tomar una decisión sobre una persona". Por ende, el foco de protección está en la creación, recolección, uso, procesamiento, exposición, almacenamiento, seguridad y transferencia de información personal de los individuos.

La organización *Privacy International* explica que lo que busca el derecho a la autodeterminación informativa es "protegerse contra el uso de poder arbitrario e injustificado, al reducir lo que se puede saber de nosotros y hacer con nosotros" (*Privacy International*, 2019). Esta mirada, que recoge el RGPD de la Unión Europea, busca devolver el control a los titulares sobre sus datos personales y lo hace a través de la exigencia de contar con el consentimiento explícito del titular para poder recolectar, tratar o transferir sus datos personales.

Sin embargo, el proceso de toma de decisión de los consumidores sobre el nivel de privacidad que están dispuestos a aceptar, es muy complejo. Como explica Acquisti (2010), los individuos son incapaces de actuar racionalmente debido a que se enfrentan a: información incompleta, una habilidad cognitiva limitada para procesar la información disponible y una multitud de sistemáticas desviaciones de la toma de decisión racional. De esta manera, "debido al fenómeno de la racionalidad limitada, un individuo es inapto para anticipar todas las consecuencias de su consentimiento y el procesamiento de datos que de él resulta" (Purtova, 2017, p.72).

Al mismo tiempo, existen diversos estudios que demuestran que las personas no toman decisiones coherentes con sus preferencias de privacidad declaradas y esa incoherencia, se conoce como paradoja de la privacidad. El estudio realizado por Motiwalla, Li y Liu (2014), buscó comprender la paradoja de la privacidad en un primer intercambio, donde individuos pueden comerciar su información personal por un valor monetario. Los resultados revelaron que la preocupación que declaran tener las personas por su privacidad no influye significativamente en el valor real que le otorgan. Por el contrario, la revelación previa del comportamiento, en situaciones específicas, es un mejor indicador del valor que le otorgan a la privacidad.

Por otro lado, las preferencias de privacidad de los consumidores muchas veces dependen de cómo fue presentada la información (*framing* o encuadre, en español). La investigación de Brandimarte, Acquisti, y Loewenstein (2013, p. 5) arrojó que la valoración de la privacidad se ve significativamente afectada por los efectos de *framing* y que el precio que le ponen las personas a la protección de su información, es diferente al precio por el cual la venderían. Los autores concluyeron que las personas están más dispuestas a recibir dinero a cambio de menor privacidad, que a pagar por más de ella. En esta paradoja, existe una relación entre la percepción de control y el comportamiento

riesgoso, mientras más control tengo sobre mis datos, es más probable que tome decisiones riesgosas.

En la misma línea, Purtova (2017, p.73) explica que "la economía del comportamiento de la privacidad, ha demostrado que el control individual y el consentimiento (el aceptar la revelación de mi información) son propensos a la manipulación, dependiendo de cómo son formuladas las condiciones de consentimiento".

La asimetría de información con respecto al uso que se les dará a los datos, sumado a la racionalidad limitada del consumidor y a la paradoja de la privacidad, cuestiona fuertemente la efectividad de las políticas regulatorias de protección de datos personales basadas en el consentimiento explícito e informado del titular. La sensación de control del titular sobre sus datos aumenta, pero no necesariamente el control real sobre ellos. Acquisti y Varian (2005) sugieren que, si los consumidores no son 100% racionales, el mercado por sí solo no puede garantizar la protección de la privacidad de los individuos.

Capítulo 2:

Protección de Datos Personales en la Unión Europea

Convención 108

La Convención de protección de datos personales de 1981 del Consejo de Europa, más conocida como la Convención 108, es el acuerdo internacional vinculante de protección de datos más importante del mundo (Greenleaf, 2018). Su objetivo, es:

> "Garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al

tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»)" (Convención 108, Artículo 1, 1981).

Adicionalmente, facilitar el libre flujo transfronterizo de datos, estableciendo como regla general el libre flujo entre territorios y como excepciones, la existencia de leyes nacionales que lo prohíban, determinadas categorías de datos de carácter personal y donde se debe comprobar que existe una protección equivalente, y cuando la transmisión hacia cierto territorio busque burlar la legislación nacional de protección de datos.

Cualquier país podía adherir voluntariamente a este compromiso y al hacerlo, debía tomar las medidas necesarias, en su derecho interno, para que se cumplieran los principios básicos. De no hacerlo, enfrentarían las sanciones que cada legislación nacional determinara, puesto que la Convención comprometía el establecimiento de mecanismos de *enforcement* para el cumplimiento de los principios.

Además de los 47 países miembros del Consejo de Europa, cinco países fuera del continente europeo adhirieron a la Convención: Uruguay, Mauritius, Senegal, Tunisia y Cabo Verde. Al mismo tiempo, Marruecos, Argentina, México y Burkina Faso, habían solicitado favorablemente el acceso y en 2018, estaban en proceso de formalizar su adherencia. Finalmente, 11 países se incorporaron a la Convención como observadores (Greeenleaf, 2018).

La fortaleza de la Convención 108, fue que sus principios fueron ampliamente aceptados en el mundo y muchas legislaciones actuales los recogen. A la vez, permitía a cualquier país adherir a la Convención y ésta, al ser vinculante, favorecía la armonización regulatoria en materia de protección de datos personales, sin afectar la soberanía de los Estados (UNCTAD, 2016).

Directiva de Protección de Datos de la Unión Europea

En 1995, la Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión Europea, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, buscó proteger de mejor forma los datos personales de los ciudadanos de la Unión Europea, al precisar y ampliar los principios de la Convención de 1981y corregir sus limitaciones. El aumento del flujo transfronterizo de datos, el surgimiento de mecanismos automatizados para el tratamiento de datos personales (no considerado en la Convención) y la necesidad de que los Estados miembro, efectivamente implementaran medidas internas para cumplir con sus compromisos en esta materia, fueron los principales problemas que buscó superar la Directiva.

La Directiva amplía y detalla las condiciones de licitud en el tratamiento de datos, en comparación al Convenio 108, y al igual que éste, permite a los Estados miembros definir en su derecho interno cómo cumplirán con esas condiciones, con la diferencia de que impone plazos a los Estados miembros para hacerlo. Es importante destacar que la legislación del Estado donde se realiza el tratamiento, o donde se ubica el responsable, es la que prevalece ante un conflicto legislativo.

La Directiva amplía la protección de los datos personales, comenzado por la recolección y abarcando todas las operaciones realizadas con los datos. Obliga a los responsables del tratamiento, a cumplir con los principios relativos a la calidad de los datos (Directiva 95/46/CE, Artículo 6), entre los cuales se exige que: el tratamiento sea leal y lícito; la recolección tenga fines determinados, legítimos y explícitos (prohibiendo un tratamiento posterior que sea incompatible con esos fines); que la recolección sea adecuada, pertinente y no excesiva (con respecto a la finalidad declarada); y que el

almacenamiento sea de datos exactos y actualizados, por un periodo de tiempo limitado a su finalidad.

La Directiva reconoce que la legitimidad del tratamiento recae en el consentimiento explícito del titular y al mismo tiempo, le otorga un especio especial al principio de finalidad para establecer si las operaciones sobre los datos personales fueron o no legítimas. Por otro lado, se prohíbe el tratamiento de datos sensibles, es decir, aquellos "que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad" (Directiva 95/46/CE, 1995, Artículo 8), con solo algunas excepciones.

La Directiva otorga una serie de derechos a los titulares de los datos: el derecho de acceso e información (incluso a conocer la lógica asociada al tratamiento automatizado de datos); los derechos de rectificación, cancelación, bloqueo y notificación a terceros (a quienes se le hayan comunicado los datos que se busca rectificar o cancelar); el derecho de oposición ciertos tratamientos de sus datos; y el derecho a no ser objeto de una decisión con efectos jurídicos, que se fundó exclusivamente en un tratamiento de datos automatizado (derecho que no contemplaba la Convención 108).

Los Estados miembros deben contar con una autoridad de control que lleve un registro de los tratamientos de datos (obliga a los responsables a informar), que evaluará los riesgos asociados al tratamiento, antes de que este tome lugar, apuntando a la máxima publicidad del tratamiento. El responsable del tratamiento, deberá reparar el daño causado a un titular por un tratamiento ilícito de sus datos, y los Estados miembro deberán determinar internamente las sanciones asociadas a este acto.

Finalmente, la Directiva busca garantizar la protección de las libertades y derechos fundamentales de las personales, con respecto al tratamiento de los datos personales, y el libre flujo transfronterizo de datos entre los Estados miembros, impidiendo cualquier restricción o prohibición a la libre circulación de los datos, con la excusa de proteger estas libertades y derechos. Por otro lado, establece que la transferencia de datos entre un Estado miembro y uno no miembro, solo se permitirá si este último garantiza un "nivel adecuado de protección" (Directiva 95/46/CE, 1995). Dentro de las excepciones a esta regla, está el consentimiento inequívoco del titular, cuando es necesario para la celebración de un contrato entre el titular y el responsable del tratamiento, y cuando existen cláusulas contractuales, que garanticen que el responsable del tratamiento ofrecerá una protección adecuada, entre otras.

En este contexto, surgen las Reglas Corporativas Vinculantes de la UE (EU *Binding Corporate Rules*, BCR), que facilitan la transferencia de datos y el cumplimiento de la legislación europea al mismo tiempo. A 2016, existían cerca de 80 compañías suscritas al BCR, 40 de ellas en Europa, 25 en EEUU y el resto de otros países, entre ellos, Japón (UNCTAD, 2016).

La Directiva, según la UNCTAD (2016):

> "Ha influido significativamente en el desarrollo global de la privacidad. Sus principios centrales aparecen de forma similar en numerosas leyes nacionales de privacidad fuera de Europa (…) y sus reglas de flujo transfronterizo de datos han fijado el estándar internacional de flujo de datos por dos décadas" (p. 32).

Reglamento General de Protección de Datos (RGPD)

El Reglamento General de Protección de Datos (RGPD), reglamento 2016/679, reemplazó a la Directiva de la Unión Europea el 25 de mayo de 2018. El RGPD actualiza la Directiva e incorpora nuevos principios y derechos, además de aumentar la responsabilidad de los controladores y procesadores sobre los datos personales que manejan.

La entrada en vigencia del RGPD, marcó la tendencia regulatoria en materia de protección de datos personales en el mercado global y forzó a otros países a seguir su modelo, o al menos a cumplir con estándares mínimos de protección de datos personales, estableciendo la necesidad de que un país sea "adecuado" para permitir el flujo transfronterizo de datos desde la Unión Europea.

El *Global Legal Group* (2018) destaca 4 aspectos clave del RGPD, siendo el primero de ellos el gran alcance que posee. La definición expansiva de datos personales[5] de la Directiva se mantiene, abarcando un gran abanico de negocios y casi todas las áreas de operación, desde el marketing a la inteligencia artificial. El RGPD abarca a los controladores y procesadores establecidos en los Estados miembro de la Unión Europea, incluso cuando el procesamiento no se realiza en la UE, y, por ende, tiene un alcance extraterritorial. El segundo punto clave, se relaciona con las penalidades asociadas al incumplimiento, las cuales alcanzan multas administrativas de hasta 20 millones de euros (o hasta el 4% de las ganancias anuales globales) para los controladores y/o procesadores que infrinjan la ley. "El RGPD parece dejar abierta la posibilidad de que las sanciones sean aplicadas tanto a los controladores como los procesadores, cuando existe un

[5] El GDPR define dato personal como "toda información relacionada a una persona natural identificada o identificable". Es identificable cuando la persona se puede identificar directa o indirectamente a través de un identificador como el nombre, la ubicación del dato u otro (GDPR, Artículo 4(1)).

incumplimiento. Este cambio tiene implicaciones serias para el negocio de los proveedores de servicios que actúan como procesadores" (Godel, Landzaat y Suter, 2017, p.3), quienes quedaban relativamente fuera del marco de acción de la Directiva.

Por otro lado, el RGPD aumenta las exigencias a los controladores y procesadores significativamente. Demanda mayor apertura y transparencia por parte de las empresas y "refuerza los límites al uso de datos personales, especialmente en el contexto de marketing directo y en ciertos tipos de perfilamiento, frente a los cuales los individuos adquieren automáticamente el derecho de oposición" (*Global Legal Group*, 2018, p.2).

El Reglamento establece siete principios que guiarán el tratamiento de datos. El principio de Transparencia, indica que el procesamiento debe ser legal, justo y transparente. Lo que implica que los controladores deben entregar información clara, accesible y concisa sobre los objetivos y alcances de la recolección y el procesamiento. El principio de limitación del propósito, señala que la recolección solo se debe realizar con un propósito legítimo, explícito y específico, y que el procesamiento que se realice no debe ser incompatible con estos. Para que el procesamiento sea legítimo, el titular de los datos debe entregar explícitamente su consentimiento, de forma libre, específica, informada y sin ambigüedades, previo al procesamiento. Un nuevo propósito de procesamiento, requerirá un nuevo consentimiento del titular. También se considera legítimo cuando el procesamiento es necesario para ejecutar un contrato del cual el titular es parte, en el cumplimiento de obligaciones legales, para proteger la vida del titular, cuando es de interés público o el ejercicio de controlador ejercido por una autoridad oficial , y cuando existe un interés legítimo por parte del controlador o un tercero (por ejemplo, conocer las preferencias de mis consumidores para poder ofrecerles mejores productos o servicios), siempre y cuando no afecte los derechos y libertades

fundamentales de los titulares de los datos. Los datos sensibles y aquellos datos relativos a menores de edad, cuentan con una protección especial.

El principio de minimización de los datos, señala que estos deben ser adecuados, relevantes y limitados al propósito de la recolección. El principio de exactitud, señala que los datos deben ser exactos y estar actualizados, por ende, obliga a tomar las medidas necesarias para corregir o eliminar los datos que no sean exactos. El principio de limitación del almacenamiento, indica que los datos almacenados permitirán la identificación del individuo solo por el tiempo que sea necesario para cumplir el propósito declarado.

El principio de integridad y confidencialidad, obliga a los controladores y procesadores a asegurar la protección de los datos personales en su poder, ante intromisiones no autorizadas, procesamientos ilegales, pérdidas accidentales, destrucción o daño, entre otros. Esto significa, que deberá establecer las medidas técnicas y organizacionales necesarias para este fin. Dentro de estas, está la obligación de contar con un Oficial de Protección de Datos. Finalmente, el principio de *accountability* (rendición de cuentas), indica que el controlador y/o procesador de datos personales, es responsable y debe ser capaz de demostrar que cumple con los principios del RGPD.

El RGPD fortalece los derechos de los individuos sobre sus datos, al ampliar algunos derechos y crear otros. El derecho de acceso del titular a sus datos se fortalece. El titular tiene el derecho a saber si el controlador tiene o no datos asociados a su persona, cuáles, quién tiene acceso a ellos, por cuánto tiempo, y si estos están siendo procesados, de qué forma y con qué fin. El titular tiene derecho a ser informado cuando sus datos son transferidos a un tercer país u organización internacional, como también de la existencia y lógica detrás de los procesos de decisión automática, junto a sus alcances. Una vez que

el titular solicita acceso a sus datos, el controlador debe entregarlos sin demora, libre de cargos (a no ser que se requieran recursos económicos excesivos) y en un formato electrónico de uso común.

El derecho a borrar o derecho al olvido (Artículo 17), representa un cambio sustancial con la Directiva y es observado como una extensión del derecho de acceso (Godel, et al. 2017), aumentando el control del titular sobre sus datos y el uso que se les da, además de poner fin a usos dañinos de los datos. Este derecho, "refleja las preferencias del consumidor y es importante al decidir si revelo o no información. Como el derecho de acceso, el derecho a eliminar datos personales es visto como una evidencia de la insatisfacción del consumidor" (Godel et al, 2017, p. 30).

La Directiva limitaba el derecho a borrar los datos, al procesamiento que causaba daño o angustia sustancial. El RGPD, amplia el derecho al permitir la eliminación cuando el dato dejó de ser necesario para el objetivo del procesamiento, cuando el titular retira su consentimiento o cuando el individuo se opone al procesamiento y no existe interés legítimo para hacerlo. Este derecho rebaja el costo de ejercerlo, al colocar en el controlador la responsabilidad de notificar a todos quienes tengan aquella información sobre la solicitud de eliminación.

También existe el derecho a rectificar mis datos personales (Artículo 16), en caso de que el titular detecte que alguno de sus datos es incorrecto, incompleto o desactualizado. El derecho a restringir el procesamiento, se da cuando el titular solicita que se corroboren sus datos personales en manos del controlador, cuando el procesamiento es ilegal y el titular se opone a la eliminación de sus datos, pero solicita restringir su uso, entre otros. En ambos casos, el controlador tiene la obligación de comunicar cualquier rectificación, eliminación y/o limitación al procesamiento, a todos

quienes se le revelaron esos datos (con la excepción de que se pruebe que es una tarea imposible por el esfuerzo desproporcionado) (Artículo 19).

El derecho a la portabilidad de los datos (Artículo 20), es el cambio legislativo más importante y el cual se espera afecte en mayor medida la relación entre el controlador de los datos y el titular (Godel et al, 2017). Se espera que la capacidad del consumidor de tomar sus datos y llevarlos a otra empresa, aumente la competencia de los mercados basados en el uso de datos personales. “El ahorro de tiempo (en ingresar datos) y la existencia de mercados secundarios de datos son los beneficios que posiblemente surgirán” (Godel et al, 2017, p.41). Esto, facilitaría el desarrollo de innovación en el uso de los datos y nuevos modelos de negocio, gracias al movimiento de los datos en control del titular. A la vez, podría reducir el costo de cambiar el proveedor de servicios. Sin embargo, existe una gran incerteza con respecto a la capacidad que tendrán los proveedores de utilizar los datos que se le transfieren, debido a la compatibilidad de formatos en los que se contengan los datos (Godel et al, 2017).

El RGPD también incorpora el derecho a objetar una decisión automática (Artículo 21) y el derecho a no ser sujeto de una decisión basada exclusivamente en un procesamiento automático de datos, incluido el perfilamiento. Finalmente, podemos señalar que toda persona tendrá derecho a retirar el consentimiento, a objetar el marketing directo y a reclamar ante una autoridad de control. Derecho de cancelación.

Es importante destacar que el RGPD permite a los Estados introducir condiciones adicionales a nivel nacional, para la protección de datos en ciertas áreas o situaciones. Por ejemplo, la edad de consentimiento de los menores de edad, va de los 13 a los 16, dependiendo el país.

El alcance territorial del RGPD se define en el Artículo 3 de la regulación y refleja la intención de los legisladores de asegurar la protección de los datos personales de los sujetos de la Unión Europea (UE) y de establecer un campo de protección nivelado para las compañías activas en mercados de la UE, en un contexto de flujo de datos a nivel mundial.

El alcance territorial del RGPD se basa en el criterio de "establecimiento" y en el de "focalización". El primer criterio, indica que la regulación aplicará sobre aquellos controladores y procesadores establecidos en la UE, incluso cuando el controlador realice el procesamiento fuera de los Estados miembro y cuando exista solo un trabajador o agente instalado en el territorio. El segundo criterio, "focalización", amplía el ámbito de aplicación del RGPD a compañías que controlen o procesen datos y que no están establecidas en la UE, dependiendo de sus actividades de procesamiento y la existencia de focalización. Las actividades se deben relacionar con la oferta de bienes y servicios (independiente de dónde se realice el pago), o con el monitoreo del comportamiento de residentes de la UE (en la UE). Para hacer esto, las compañías deberán designar a un representante en la UE, el cual deberá facilitar la comunicación entre el titular de los datos, la autoridad de control y el controlador o procesador. Esta figura, se creó para garantizar el cumplimiento del RGPD (European Data Protection Board [EDPB, 2018).

La transferencia transfronteriza de datos personales, se podrá realizar solo entre los países sujetos al RGPD y hacia aquellos que hayan sido catalogados como "adecuados" por la Comisión Europea, en base al artículo 45 del RGPD. Para esto, se evalúa la legislación existente, las autoridades de control y los acuerdos internacionales relacionados. Ante las nuevas exigencias del RGPD "varias jurisdicciones que actualmente se benefician de la "adecuacidad" otorgada por la Comisión Europea, están actualizando sus leyes nacionales de protección de datos" (Godel et al, 2017, p.3).

La regulación obliga a las empresas y a los Estados a proteger los datos personales y la privacidad de los residentes de la UE, por lo que posee un alcance jurisdiccional extraterritorial que podría afectar el comercio internacional, al limitar o prohibir el flujo transfronterizo de datos.

Convención 108 +

Con la entrada en vigencia del RGPD, el Consejo de Europa adoptó un protocolo modificativo que actualizó la "Convención 108" y que incorporó nuevas obligaciones y derechos. La Convención 108+, como se conoce: incorpora la obligación de las organizaciones de notificar cualquier brecha de seguridad sobre los datos[6] y el derecho a recibir una compensación en caso de una vulneración; aumenta las exigencias de transparencia en el procesamiento de datos, al establecer nuevos derechos de los titulares, entre ellos, el no ser sujeto de una decisión que se basó exclusivamente en el procesamiento automatizado de datos y el derecho a oponerse al tratamiento.

La modernización de la Convención, refuerza la protección de los datos sensibles, especifica aún más el principio de tratamiento lícito y fortalece el derecho de los titulares de sus datos, especialmente en torno al acceso y a la transparencia del tratamiento. Garantiza un alto grado de protección y al mismo tiempo, otorga flexibilidad a los países en la implementación de medidas en su ordenamiento jurídico interno.

Por otro lado, modifica el artículo que regula la transferencia transfronteriza de datos personales y declara que los países sujetos a la Convención no deben prohibir o condicionar a una autorización especial, la transferencia de datos hacia otros países que

[6] Los controladores y los procesadores deben tomar las medidas de seguridad necesarias para la protección de los datos personales que tienen en su poder, y notificar oportunamente (al menos a la autoridad de control) cualquier brecha de seguridad que pueda interferir con los derechos y libertades fundamentales de los titulares.

sean parte de la Convención (no así, hacia aquellos que no lo sean). La excepción a esta regla, se da solo cuando existe un real riesgo de que la transferencia permita eludir las obligaciones de la Convención o cuando el país haya adherido a reglas de protección armonizadas y compartidas por diferentes Estados pertenecientes a una organización internacional o regional. Cuando el país no es parte de la Convención, se permitirá la transmisión de datos solo cuando éste ofrezca un nivel adecuado de protección, ya sea a través de la legislación nacional, la adhesión a acuerdos internacionales o los acuerdos legalmente vinculantes y ejecutables, entre otros.

Finalmente, obliga a los países miembros a establecer al menos una autoridad de control responsable del cumplimiento de la Convención, con poder para investigar, intervenir, imponer sanciones administrativas y comenzar acciones judiciales. Esta autoridad, debe ser independiente e imparcial en su labor, además de permitir la apelación de sus decisiones en la Corte. La labor del Comité de la Convención se fortalece, al obligar a los países a someterse a una evaluación de efectividad sobre las medidas implementadas para dar cumplimiento a la Convención.

La modernización de la Convención 108, o 108+, finalizó el 18 de mayo de 2018, y solo los países miembros pertenecientes a la Unión Europea, podrán ratificar su adhesión una vez que cumplan con los nuevos estándares. El Comité de Ministros del Consejo de Europa, debe aún decidir si permitirá la adhesión de países que no pertenecen a la UE y esto solo podrá hacerlo, si los miembros de la Convención alcanzan un acuerdo unánime.

La Convención 108+ se ajusta a los requerimientos relativos al tratamiento de datos personales y al flujo transfronterizo de estos, del RGPD. La adhesión a la Convención, será un factor determinante a la hora de establecer si un país es adecuado o

no en el marco del RGPD. Para Greenleaf (2018), la Convención 108+ podría convertirse en el mecanismo de armonización regulatorio más importante del mundo, porque garantiza una alta protección sobre los datos personales, cumple con los estándares del RGPD, la Directiva de la UE, el marco de privacidad de la APEC, las Directivas de la OCDE y al mismo tiempo, garantiza la soberanía de los países al otorgar flexibilidad en las medidas internas a implementar para cumplir con la Convención.

Impacto económico del GDPR

La *European Data Protection Board* [EDPB], (2019), realizó un balance del RGPD a un año de su entrada en vigencia y expuso que, entre mayo de 2018 y junio de 2019, las autoridades de protección europeas reportaron 95.180 casos de quejas de individuos que consideraron sus derechos fueron vulnerados, principalmente en el área del telemarketing, los mails promocionales y la videovigilancia. Por otro lado, informó que se recibieron 41.502 notificaciones de violación de seguridad de los datos.

En el año de vigencia del RGPD, el EDBP (2019) observó varios casos de alto nivel y que podrían ocasionar multas por su máximo, y destaca los siguientes: multa de Alemania a una red social, por fallar en asegurar los datos de sus usuarios (20 mil euros), multa de Austria (5.280 euros) a un café por videovigilancia ilegal y multa de Francia a Google con 50.000.000 euros por la falta de consenso en sus anuncios.

Con respecto a la implementación del RGPD en la UE, es importante destacar que a junio de 2019 aún estaba pendiente la adaptación de la legislación nacional al RGPD de Bulgaria, Grecia, Eslovenia, Portugal y República Checa, lo que podría ser un indicio de las dificultades que enfrentan los países para su implementación (EDBP, 2019).

Sobre el aspecto institucional, la EDPB (2019), advierte que las autoridades de control destinan tiempo y recursos en facilitar esta cooperación, lo que podría afectar el

presupuesto de los reguladores. De hecho, señalan que la mayoría de las autoridades de control ampliaron su presupuesto entre 2018 y 2019. Donde 17 de 26 autoridades solicitaron entre un 30-50% más, además de ampliar su equipo. La cooperación entre autoridades se dio en casos de flujo transfronterizo de datos y ante el alegato de un individuo.

En los primeros nueve meses de vigencia del RGPD las autoridades de control de 11 países establecieron multas por 55.955.871 euros. A la vez, se registraron 281 casos con componente de transferencia transfronteriza de datos, 194 de ellos originados por alegatos de individuos, principalmente relacionados con el ejercicio de derechos del titular, asociados a los derechos del consumidor e infracciones de seguridad de los datos.

Desde la entrada en vigencia del GDPR se han realizado diversos estudios que buscan dimensionar el impacto económico que tendrá esta regulación en los mercados europeos. El estudio de (Allen, Berg, Berg, Markey-Towler y Potts, 2018) explora cómo la regulación cambia el valor de los datos y cuál es el impacto potencial en ese mercado. La tesis principal, es que el derecho de los titulares a retirar su consentimiento en cualquier momento (derecho de cancelación), implica que el valor de los datos en poder del controlador (que busca venderlos a un tercero) puede llegar a cero o ser incluso negativo. Si el titular retira el consentimiento y los datos persisten, el controlador corre el riesgo de multas, y si lo elimina, el proceso tiene un costo asociado. Por otro lado, la incerteza sobre el valor de los datos podría afectar a las empresas que ofrecen servicios gratis a los usuarios y basan su modelo de negocio en la recolección y venta de datos con fines de microtargeting (Allen et al, 2018).

Para Blades y Herrera (2016) el derecho de cancelación limita fuertemente los derechos de propiedad del controlador sobre los datos y los coloca en manos del titular.

Como las firmas invierten recursos en almacenar y procesar la información, sería un desincentivo a la inversión, puesto que aumenta la incerteza. En este escenario, el perfil de riesgo de los controladores y procesadores de datos cambia y surge el incentivo de tomar un seguro contra el riesgo de que el titular de los datos retire su consentimiento, y los datos pierdan su valor en el futuro, siempre y cuando la pérdida esperada sea mayor al costo del seguro. Por ende, este aspecto de la regulación "incentiva la expansión de mercados financieros al extender servicios para compartir el riesgo" (Allen et al, 2018, p.6), como también, podría provocar la reducción de oferta a residentes europeos.

El estudio realizado por Wallace y Castro (2018), plantea que el nuevo reglamento europeo de protección de datos personales, tendrá un impacto negativo sobre el desarrollo y uso de Inteligencia Artificial (IA) en Europa, colocando a las empresas en desventaja competitiva frente a sus competidores de Norteamérica y Asia (con regulaciones menos estrictas). Por lo tanto, el RGPD sería un freno para el desarrollo de la economía digital en los próximos años, al limitar el uso que se les da a los datos con estos fines y aumentar el riesgo legal para las compañías al hacerlo.

Por otro lado, la obligación de que las empresas revisen manualmente las decisiones de algunos algoritmos, aumentaría significativamente los costos de capital humano, desincentivando el uso de IA (que busca automatizar funciones para hacerlas más rápidas y menos costosas de lo que lo hubiera hecho un humano). Para Blades y Herrera (2016), el derecho a no ser sujeto de una decisión que se basó únicamente en un procesamiento automático, incluido el perfilamiento, reduce el valor de los datos, al limitar las posibilidades de su explotación, y, por ende, desincentiva el desarrollo e innovación de algoritmos.

Al mismo tiempo, el derecho de los titulares a borrar sus datos puede dañar los sistemas de IA, especialmente cuando utilizan *machine learning*, puesto que el sistema aprende de los datos que va recolectando y eliminar la existencia de algunos de esos datos, puede provocar fallas en el sistema, arrojando resultados imprecisos o incorrectos. Esto limitaría el beneficio de los otros titulares de datos o incluso, hacerlo inexistente (Wallace y Castro, 2018).

El principio de finalidad, que prohíbe el uso de datos para otros fines para los cuales fue recolectado, limitaría la capacidad de innovación de las empresas que utilizan IA para experimentar nuevas funciones que podrían mejorar sus servicios, afectando al negocio y a los consumidores. Al mismo tiempo, la obligación de obtener consentimiento cada vez que se quiera dar un nuevo uso a los datos recolectados, aumenta los costos del tratamiento y desincentiva la innovación (Wallace y Castro, 2018).

Para estos autores, el RGPD limitaría el surgimiento de compañías en la UE de Inteligencia Artificial, además de reducir el uso de esta herramienta en empresas de la UE. Esto además impactará el comportamiento de las compañías extranjeras, que tendrán menos incentivos para ofrecer productos de IA en UE, haciendo de este mercado uno menos competitivo e innovador.

Jia, Zhe Jin y Wagman (2018) estudiaron el impacto a corto plazo del RGPD en la inversión en nuevas y emergentes firmas tecnológicas en la UE, en comparación a EEUU (con una regulación menos estricta) y descubrió que "el GDPR afectó negativamente al número de acuerdos relacionamos a emprendimientos (*ventures*), el tamaño de estos acuerdos y el total de dólares invertidos en cada uno de ellos" (Jia, et al. 2018, p.20), mostrando efectos diferenciales negativos en los emprendimientos de la UE en comparación a EEUU. El estudio observó una reducción del 17,6% del número de

acuerdos semanales, una baja de 39,6% en el monto recaudado promedio por acuerdo y estima una potencial pérdida que va entre los 3.604 y 29.819 de puestos de trabajo que se habrían generado por estos emprendimientos. El efecto negativo más fuerte se daría en emprendimientos entre 0 y 3 años.

El RGPD aumentará el costo de las empresas que utilicen datos personales, puesto que requerirá de personal y tecnología especializada para cumplir con sus exigencias (Wallace y Castro, 2018). Por ejemplo, el derecho de acceso, implica diseñar y mantener sistemas y procedimientos para permitir el acceso a los datos de su titular (Blades y Herrera, 2016). De esta forma, podemos observar que la regulación que busca la protección de los datos personales en la UE, podría generar barreras de entrada y afectar la innovación.

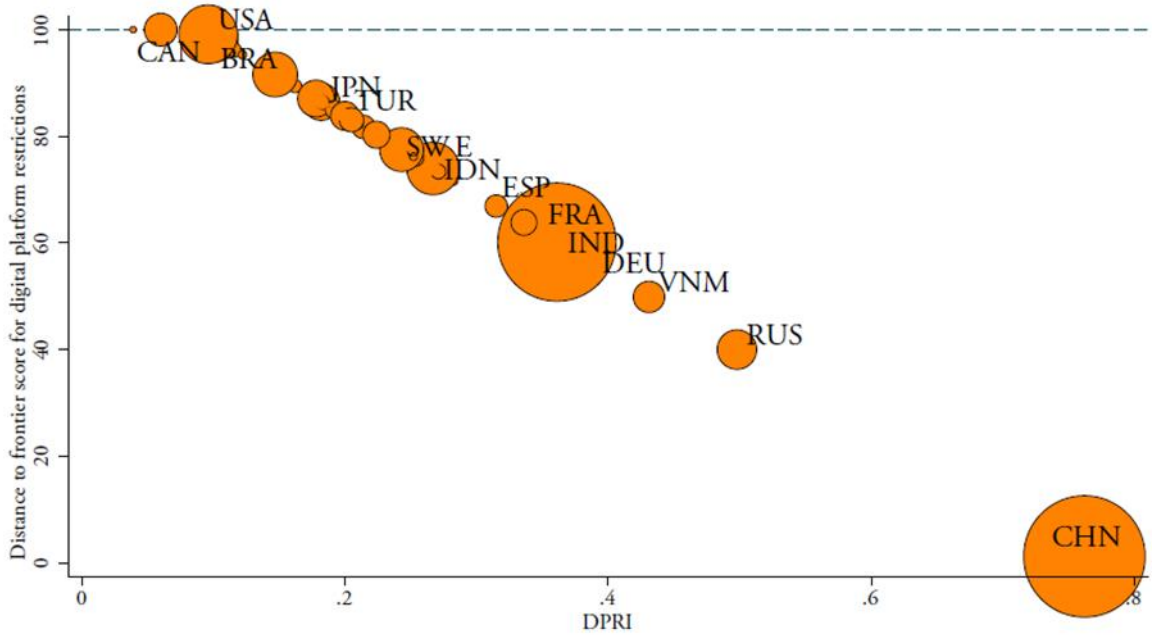
Por otro lado, Wallace y Castro (2018), plantean que la prohibición de transferencia transfronteriza de datos fuera de la UE, con la excepción de aquellos países calificados como "adecuados", restringe innecesariamente el lugar donde las organizaciones almacenan los datos. Esto hace que los servicios de nube sean menos competitivos y distorsiona el costo de la IA, aumentando su precio. Por otro lado, indican que las multas del RGPD golpearán más fuerte a las pequeñas empresas, porque las grandes nunca pagarán el 4% real, porque existe el tope de 20 millones de euros, algo que para un emprendimiento puede significar quedar fuera del negocio.

Como aspecto positivo del RGPD, Wallace y Castro (2018) destacan que el derecho a la portabilidad de los datos estimulará la competencia en IA en la UE, porque facilitará que los consumidores compartan sus datos con nuevas compañías que necesitan de ellos para entregar un servicio. Sin embargo, advierten que la legislación no mide adecuadamente el costo y la factibilidad de transferir bases de datos extremadamente

grandes y complejas, por lo que no queda claro si la portabilidad será factible. Blades y Herrera (2016) agregan que este derecho facilita el cambio entre un proveedor y otro, bajando el costo de adquisición de nuevos datos personales, favoreciendo la competencia.

Ferracane y van der Marel (2018), plantean que las plataformas en línea enfrentan niveles crecientes de regulación en el mundo y que, en algunos casos, esto podría afectar su potencial de crecimiento y, por ende, los beneficios económicos derivados de los efectos de red. Las restricciones regulatorias corresponderían a aquellas que restringen el uso doméstico de los datos y el movimiento transfronterizo de datos, aumentando el costo de hacer negocios en el extranjero. El estudio desarrolló un índice de política de datos que mide cuán restrictivo es un país y los resultados arrojaron que cuatro de los ocho países más restrictivos pertenecen a Europa y que las restricciones a las plataformas en línea se asocian significativamente con menores contribuciones del sector de las Tecnologías de la Información y Comunicaciones (TIC) y al crecimiento productivo de la economía en general. Utilizando este índice, estimaron el efecto de estas políticas en la importación de servicios ofrecidos en línea y encontraron que “las políticas de datos más restrictivas, particularmente con respecto al flujo transfronterizo de datos, resultan en menores importaciones de servicios con uso intensivo de datos en los países que las imponen” (p.15).

Figure 2.2: Distance to the regulatory frontier for platform restrictions (overall)



Fuente: Ferracane, M.F. & van der Marel, E. (2018b, p.7).

El estudio de Cory (2017) va en línea con este resultado e indica que "las grandes firmas de EEUU señalaron a Europa como el área donde la privacidad de los datos y los requerimientos de protección, representan los mayores obstáculos para hacer negocios en línea" (p.23).

Capítulo III:

Protección de Datos Personales en el Mundo

La entrada en vigencia del Reglamento General de Protección de Datos (RGPD) de la Unión Europea, en 2018, y con alcance extraterritorial, motivó el surgimiento de iniciativas legales de protección de datos personales en todo el mundo y reveló la necesidad de contar con regulaciones compatibles entre sí a nivel nacional e internacional, para asegurar la protección de datos personales y facilitar, y potenciar, el comercio global simultáneamente.

En 2016, el 55% de los países del mundo contaba con una legislación en esta materia, el 18% tenía un proyecto de ley y el 13% no tenía ni ley ni proyecto (el 26% restante no entregó información). Este escenario, reduce la confianza sobre una amplia gama de actividades comerciales y dificulta en gran medida, la participación de casi un tercio de los países del mundo en la economía digital (UNCTAD, 2016).

Las iniciativas internacionales que buscan armonizar las diferentes regulaciones en materia de protección de datos personales tienen larga data y se han ido actualizando con el tiempo. A continuación, revisaremos brevemente las más relevantes del mundo.

Lineamientos de Privacidad OCDE (OECD Privacy Framework) 2013

El 11 de julio de 2013, la OCDE adoptó la recomendación revisada de los lineamientos para la protección de la privacidad y el flujo transfronterizo de datos personales, originada en 1980. La guía revisada, busca abordar la protección de la privacidad desde el manejo del riesgo (incorpora el término de "notificación de brecha de seguridad de los datos") y apunta a hacerse cargo de la dimensión global de la privacidad, reconociendo la necesidad de mejorar la interoperabilidad y evidenciar que la disparidad de las legislaciones podría generar barreras para el libre flujo de datos transfronterizo (OCDE, 2013).

La guía publicada en septiembre de 1980, tiene 8 principios y representa "la primera declaración internacional acordada sobre los principios de privacidad de la información esenciales, que reflejan las diversas miradas y perspectivas de los países en el mundo", (OCDE, 2013, p.76). Lo que busca es generar un compromiso entre sus miembros para fijar principios básicos de protección, con atención al legítimo interés de los países por prevenir transferencias de datos que puedan atentar contra su seguridad, el

orden público o ser contraria a su legislación nacional, como también aquellas que violan los derechos de sus ciudadanos.

Los principios de la OCDE, como veremos a continuación, son bastante consistentes con los del Reglamento Europeo. El principio de limitación de la recolección, se relaciona con el principio de calidad de los datos (en el mismo sentido que utiliza la Convención 108 descrita previamente), el propósito del procesamiento (que debe ser legítimo y respetar los derechos civiles), la limitación de las acciones de recolección de datos para ciertos controladores y los métodos de recolección de datos utilizados (prohibiendo el uso de mecanismos de recolección invisible para el usuario). "El conocimiento o consentimiento del titular de los datos es como regla esencial, siendo el conocimiento el requisito mínimo" (OCDE, 2013, p.56).

El principio de especificación del propósito está asociado a los dos principios anteriores (calidad y limitación de uso) y apunta a que antes, o durante, el momento de recolección de los datos, debe ser posible identificar los propósitos. Agrega que el propósito puede cambiar, siempre que sea compatible con los fines iniciales y sea comunicado al titular de los datos. A la vez, el principio de limitación de uso indica que los datos solo deben ser utilizados y compartidos con los fines y entidades especificadas, con la excepción del consentimiento del titular y la autoridad legal.

Por otro lado, establece el principio de seguridad, apuntando a que los controladores tomen las medidas de seguridad necesarias para la protección de los datos. Además, la guía expone que, si el dato ya no sirve para el propósito declarado, debe ser destruido o anonimizado.

Dentro de los principios más importantes, está el de apertura y de participación individual. Es el derecho de acceder a mi información personal en manos de un

controlador, el cual debe ser fácil de ejercer y en un tiempo razonable. Finalmente establece el principio de *accountability* (rendición de cuentas), estableciendo que el controlador de los datos es responsable de la seguridad de los datos, incluso cuando externaliza la tarea de procesamiento, y que deben existir sanciones legales o códigos de conducta, como mecanismos de *enforcement* (aplicación o ejecución).

El flujo transfronterizo de datos, de forma segura e ininterrumpida, se permite cuando el país de destino cumple con los requerimientos de esta guía. Los principios guía de la OCDE (2013), reconocen "el valor económico de la información y la importancia de proteger el "comercio de datos" con reglas aceptadas de libre competencia" (p.44), junto con la necesidad de establecer medidas de seguridad que minimicen la violación de la propiedad de los datos y el mal uso de la información personal.

Casi la totalidad de los países miembro de la OCDE tienen legislación para la protección de los datos personales y autoridades de control para su cumplimiento (OCDE, 2013), pero no todos siguen los lineamentos de la guía puesto que esta no posee carácter vinculante. Un ejemplo de ello es Chile, país que ingresó a la organización en 2010 y asumió el compromiso de implementar los lineamientos relativos a la protección de la privacidad y el flujo transfronterizo de datos personales. Viollier (2017, p. 39) señala que esta obligación "luego de reiteradas solicitudes de aplazamiento, a la fecha no se ha cumplido, lo que le ha valido a Chile ser objeto de advertencias por parte del organismo".

Los lineamientos de la OCDE no son vinculantes y esa es su principal debilidad. A la vez, y a diferencia de la regulación europea, la guía no incorpora el principio de "proporcionalidad", no protege de forma especial el tratamiento de datos sensibles y no aplica los principios, al procesamiento automático de datos.

Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico (APEC)

El Foro de Cooperación del Asia-Pacífico (APEC, por sus siglas en inglés) es una organización multinacional que busca promover el crecimiento económico, la cooperación, el comercio y la inversión en la Región Asia-Pacífico, del cual Chile forma parte desde 1994. El 64% del intercambio comercial de nuestro país se realiza con esa región y esta recibe el 69% de nuestras exportaciones (Dirección General de Relaciones Económicas Internacionales [DIRECON], 2018). En 2019, Chile fue sede de este foro, que tiene entre sus prioridades la sociedad digital y la integración 4.0.

Los lineamientos de la APEC sobre privacidad están fuertemente influenciados por los de la guía de la OCDE y son consistentes con sus lineamientos. Incluso en 2015, la APEC actualizó su Marco de Privacidad e incorporó los cambios que realizó la OCDE a sus lineamientos en 2013. Además, 7 de las 21 economías de la APEC son miembros de la OCDE.

Las economías miembros de la APEC, "reconocen el gran potencial de la economía digital para expandir las oportunidades de negocios, reducir los costos, aumentar la eficiencia, mejorar la calidad de vida y facilitar una mayor participación de los pequeños negocios en el comercio global" (APEC, 2015, p. 4). En este contexto, se evidencia la necesidad de contar con un marco legal de protección de la privacidad que sobrepase las fronteras y permita las transferencias regionales de información personal, en beneficio de los consumidores, los negocios y gobiernos.

Los lineamientos de la APEC apuntan a que las regulaciones en materia de protección de datos personales sean consistentes, más que idénticas, apuntando a establecer un mecanismo regional para promover y hacer cumplir el derecho a la protección de los datos personales. Este mecanismo es el *Cross Border Privacy Rules* (CBPR), acuerdo voluntario firmado en 2011 por los países miembro de la APEC y que

busca: fijar un criterio para los órganos nacionales encargados del cumplimiento de la protección de datos (autoridades de control) y también para los controladores de información (los cuales voluntariamente deben pasar por un proceso de certificación); asentar criterios de cumplimiento del sistema CBPR para las autoridades de control sobre los controladores de información; y acuerdos para hacer cumplir el sistema, a través del proceso de reclamos (APEC, 2015).

El CBPR es un sistema basado en la autorregulación, donde compañías se adhieren voluntariamente al solicitar certificación al *Accountability Agent* (agente de cumplimiento), pagando una cuota anual. En 2016, había solo 4 economías participando: Canadá, Japón, México y EEUU (UNCTAD, 2016). Adicionalmente, surge el CPEA (*Cross-border Privacy Enforcement Arrangement*), mecanismo multilateral práctico que permite a las autoridades de control cooperar en el cumplimiento de los lineamientos cuando se produce un flujo transfronterizo de datos, al crear un marco bajo el cual las autoridades pueden, voluntariamente, compartir y solicitar información, además de otorgar asistencia.

Los principios del marco de protección de datos de la APEC son: la prevención del daño (evitando el mal uso de la información personal), estableciendo obligaciones específicas para enfrentar el riesgo y medidas para subsanarlo; la notificación clara de las políticas de privacidad por parte de los controladores (que debe comunicar el objetivo de la recolección, organizaciones que tendrán acceso a los datos, la identidad, ubicación y contacto del controlados), además de permitir el acceso del titular a sus datos personales y su corrección. La notificación idealmente se debe realizar antes o en el momento de la recolección, pero la APEC reconoce que no siempre es posible (pensemos en el caso de las *cookies*).

También existe el principio de limitación de la recolección, a aquella información que es relevante para su propósito, junto con exigir que los mecanismos de recolección sean legales y a través de medios justos. Se limita también el uso de los datos, para los fines que fueron recolectados u otros propósitos relacionados, siempre que exista consentimiento, sea necesario para proveer un servicio o producto que solicita el individuo, y una autoridad de la ley lo requiera con efectos legales. Por otro lado, promueve la elección sobre la recolección, uso, transferencia y exposición de los datos por parte del titular, con mecanismos claros y accesibles para ejercer la elección sobre estos ítems; la integridad de la información y su seguridad; el acceso y corrección de la información por parte de su titular, siempre y cuando no genere problemas legales o de seguridad, cuando el costo de realizar la acción sea demasiado alto comparado con el riesgo y cuando afecte los derechos de terceros. Finalmente, está el principio de *accountability*, donde el controlador es responsable de implementar los principios antes mencionados.

Las principales limitaciones del marco de protección de datos personales de la APEC se relacionan con la soberanía nacional, la seguridad nacional, seguridad pública y políticas públicas. Sin embargo, las excepciones deben ser limitadas y proporcionales a la consecución de los objetivos que buscan, además de ser de público conocimiento y acorde con la ley (APEC, 2015). El objetivo, es promover la interoperabilidad de las regulaciones de privacidad entre los países miembro. Sin embargo, solo una cantidad limitada de países ha adherido a esta iniciativa, lo que hace que su alcance sea más bien limitado, además de ofrecer un estándar de protección menor que el consagrado en los documentos de la OCDE.

Acuerdo Transpacífico de Cooperación Económica [TPP]

El Acuerdo Transpacífico de Cooperación Económica (TPP, por sus siglas en inglés), estipula que cada estado miembro debe adoptar un marco legal "que disponga la protección de la información personal de los usuarios del comercio electrónico" (Salas, 2018, p.121-122). En este caso, información personal es cualquier información o dato sobre una persona natural identificada o identificable. El TPP señala la necesidad de establecer un balance entre la protección de datos personales y el comercio. Limita el alcance de la legislación nacional en esta materia, siguiendo el acuerdo general sobre el comercio de servicios de la Organización del Comercio Mundial (*World Trade Organization*) (UNCTAD, 2016).

Sólo permite restricciones en el flujo transfronterizo si sucede que: la ley es necesaria para alcanzar objetivos legítimos de política pública, la ley no sea aplicada de forma arbitraria y/o discriminatoria injustificadamente, la ley no debe imponer restricciones al comercio y que la ley no imponga restricciones a la transferencia de información más grandes que las requeridas para lograr el objetivo (UNCTAD, 2016).

Además, exige que los miembros permitan la transferencia transfronteriza de datos por medios electrónicos, incluso la información personal, cuando el objetivo de esto sea "la realización de un negocio de una persona cubierta".

Los principios de protección de datos comunes incluyen la existencia de una razón legítima para el procesamiento de datos, obtenida a través del consentimiento directo u otra justificación en base al interés público, la calidad de los datos (precisos, completos y vigentes), y la seguridad de los datos (UNCTAD, 2016).

Chile se sumó al acuerdo TPP en 2015 y este será vinculante una vez que los 12 países que lo integran lo ratifiquen (UNCTAD, 2016).

Tres grandes reinos de datos

Pese a las diversas iniciativas internacionales que buscan armonizar la regulación en materia de protección de datos personales, la realidad es que tenemos un sistema internacional fragmentado. Algunos sistemas protegen la privacidad como un derecho fundamental, otros lo hacen desde una mirada constitucional, como un derecho del consumidor y otros, simplemente no lo hacen. Algunas regulaciones aplican igual a todos los sectores, y otras, tienen reglas diferentes para sectores específicos, tipo de entidad de procesamiento o categoría de datos (sensibles o de menores). Unos sistemas operan en base a acciones de *enforcement* iniciadas por individuos o su grupo de representación y otras entregan el poder de control a una autoridad supervisora especializada, mientras que algunas mezclan un poco de ambas. Esta situación, genera incertidumbre, y desconfianza, en los consumidores y productores de todo el mundo (UNCTAD, 2016).

En este contexto, Aaronson y Leblond (2018) plantean la existencia de tres grandes "reinos de datos": Estados Unidos (EEUU), China y la Unión Europea (UE). Donde cada uno de ellos, ha adoptado diferentes estrategias buscando crear un ambiente propicio para impulsar el desarrollo nacional de los sectores económicos impulsados por los datos y posicionarse como líderes mundiales en la materia. "Dada su ventaja comparativa en estos nuevos sectores impulsados por los datos, su inversión temprana y gran cuota de mercado, los tres reinos fijan las reglas del flujo de datos" (p.3). Los autores plantean que, para mantener su posición dominante, estos países necesitan acceder a la mayor cantidad de datos posible y para ello, buscan adherir a su reino a otros países, a través de incentivos (acuerdos comerciales) o técnicas de coerción (como condicionar el acceso al mercado al seguimiento de ciertas reglas).

Estados Unidos posee una ventaja comparativa en los sectores económicos impulsados por los datos y sus políticas regulatorias apuntan a proteger esta ventaja. El libre flujo transfronterizo de los datos es su prioridad y "utilizan los acuerdos comerciales para desarrollar economías de escala y alcance en datos, y prohibir prácticas, como los requerimientos de localización de datos y servicios, que puedan distorsionar el comercio" (Aaronson y Leblond, 2018, p.3). En el lado opuesto, la Unión Europea basa su reino en la protección de los datos personales, en el convencimiento de que la confianza es clave para que los ciudadanos permitan que las empresas utilicen sus datos personales y se pueda desarrollar todo el potencial de la economía digital. Finalmente, el reino de datos de China establece sus políticas apuntando a mantener la estabilidad social, el poder del partido comunista y el desarrollo de sectores basados en el conocimiento y los datos, como la inteligencia artificial. Con esto en mente, restringen fuertemente el libre flujo nacional y transfronterizo de datos personales (Aaronson y Leblond, 2018).

Los tres principales mercados digitales del mundo, EEUU, China y la UE, abordan la transferencia transfronteriza de datos de diferentes formas. Esto genera un problema para el resto de los países, quienes deberán enfrentar un alto costo regulatorio, al aumentar el costo de *compliance* (ante diferentes estándares). Las ganancias de los sectores impulsados por los datos probablemente se concentrarán en China y EEUU, debido al círculo virtuoso del sector y a que estos países ya poseen el talento, la cuota de mercado y los datos para ponerlo en marcha. Los países desarrollados tienen poco espacio para capturar datos y, por ende, ganar ventajas comparativas en la economía guiada por los datos.

A continuación, revisaremos las principales características de los tres reinos digitales. Comenzaremos brevemente con China, destacando su posición dominante y las políticas que apuntan a fortalecerla. Debido a que el modelo chino se sustenta en el acceso

a un gran mercado de datos personales nacional y en un sistema político centralizado y proteccionista, no ahondaremos en éste, debido a que este modelo no es factible de imitar por Chile. Continuaremos con EEUU con mayor profundidad, debido a la influencia histórica que ha tenido el modelo neoliberal en nuestro país y finalizaremos con la Unión Europea, donde ya hemos realizado un análisis más profundo, debido a que es este modelo el que busca imitar Chile en su proyecto de ley que busca actualizar la regulación de protección de los datos personales.

El reino de datos de China

China es el país que posee más usuarios de internet a nivel mundial, con 854 millones, a junio de 2019, tiene más del doble de usuarios que Estados Unidos, que se ubica en el tercer lugar con cerca de 293 millones (Clement, 2020). China posee 7 de las 30 compañías más importantes de internet capitalizadas en el mercado, dentro de las cuales se encuentra Alibaba (402 miles de millones de dólares) y Tencent (398 miles de millones de dólares) en el top ten (Meeker, 2019). El Foro Económico Mundial, expuso que, en 2018, de las 608 patentes relacionadas a Inteligencia Artificial registradas, China fue responsable de 473, y que un tercio de las iniciativas llamadas unicornio (compañías que valen más de mil millones) en el mundo, provienen de China (Broom, 2019).

"Con una gran población de consumidores y un estándar relativamente bajo de protección de datos, China ofrece a sus firmas un ambiente atractivo para desarrollar nuevos productos y servicios digitales, especialmente en Inteligencia Artificial", (Aaronson y Leblond, 2018, p. 25). El gobierno chino tiene la capacidad de acceder a todos los datos personales en manos del sector público y privado, lo que le ha permitido al país alcanzar rápidamente economías de escala y alcance, y, por ende, impulsar el desarrollo de Inteligencia Artificial en las firmas.

El gobierno regula el acceso a internet y es dueño de la infraestructura que lo habilita. Al mismo tiempo, juega un rol activo en la inversión, desarrollo y consumo de servicios y productos digitales. Eso sí, "la innovación de China ocurre bajo el "*greate firewall*", un sistema de censura, filtros y requerimientos tecnológicos establecidos por el Partido Comunista Chino" (Aaronson y Leblond, 2018, p.18). El contenido de Internet está fuertemente regulado y no existe expectativa de protección a la libertad de expresión.

Las fuertes regulaciones en materia de datos personales, que restringen y condicionan el flujo, almacenamiento y procesamiento de datos, son reconocidas como medidas de proteccionismo digital por Cory (2017). Este autor, plantea que China posee una de las más amplias políticas de requerimiento de localización de datos (obligación de almacenar y/o procesar los datos en territorio nacional), que impiden el flujo de datos entre China y el resto del mundo. El autor, señala entre ellas:

- En 2011 China prohibió el almacenamiento y procesamiento de datos personales financieros fuera del país.
- En 2013, requirió que toda la información crediticia de los ciudadanos chinos fuera almacenada y procesada en el territorio.
- En 2016, forzó a las compañías de internet que entregaban servicios de mapeo, a almacenar sus datos localmente.
- En 2016, estableció que las firmas extranjeras que ofrecen servicios de almacenamiento computacional en la nube, solo pueden operar si un socio chino posee al menos el 50% del negocio.
- En 2017, estableció que las empresas con información de infraestructura crítica y operadores de red, que quisieran transferir datos transfronterizamente, debían

solicitar autorización al gobierno y este podía negarla, si consideraba que podría significar un riesgo para la seguridad de la nación o su sistema político.

Todas estas políticas restringen el acceso al mercado chino y son consideradas por Cory (2017), como políticas discriminatorias hacia las compañías extranjeras y que buscan potenciar el desarrollo nacional de un sector tecnológico. En la misma línea, Aaronson y Leblond (2018), plantean que China restringe el flujo de datos personales transfronterizamente y a nivel nacional, con el argumento de resguardar la seguridad nacional y mantener la estabilidad social. Sin embargo, estas políticas restrictivas y discriminatorias sirven para mantener el poder del partido comunista y para facilitar el surgimiento de campeones nacionales chinos, al reducir la competencia del exterior.

China no posee una ley de protección de datos personales y lo más cercano a una regulación en esta materia, es la ley de Ciberseguridad publicada en 2016 (DLA Piper, 2019). Esta ley, principalmente fortaleció el requerimiento de localización de los datos, estableció que la información personal debe ser almacenada en China y que para tratar datos personales se debe contar con el consentimiento del titular. Por otro lado, limitó la transferencia transfronteriza de datos a la autorización del gobierno y al consentimiento del titular, y estableció la obligación de notificar incumplimientos de seguridad de los datos. En 2018, China publicó el Estándar Nacional para la Protección de Datos Personales, que se encuentra en el cuarto sistema de la Ley de ciberseguridad. Este estándar, son buenas prácticas para el almacenamiento, procesamiento y transferencia de información sensible, por ende, no es obligatorio. La eliminación de datos a solicitud del titular se recomienda, pero la ley de ciberseguridad indica que todos los datos personales siempre se deben guardar por si el gobierno los necesita para realizar alguna investigación (DLA Piper, 2019).

Las penalidades por violar la ley de Ciberseguridad, van entre los 7.500 y 75.000 dólares y pueden significar la revocación de la licencia o permiso del negocio. Incluso, los operadores de red pueden enfrentar entre 5 y 15 días de prisión al violar ciertas reglas.

El reino de datos de Estados Unidos

Desde que el uso de internet se expandió a nivel mundial en los años 90, Estados Unidos ha liderado la economía impulsada por los datos. Siete de las diez compañías de internet más valiosas del mundo provienen de EEUU, dentro de las cuales se encuentran Amazon, Apple, Facebook, Google, Intel y Microsoft (Statista, 2019). Mientras que más de la mitad de la capacidad de almacenamiento computacional en la nube (*Cloud computing*) a nivel mundial, proviene de cuatro compañías estadounidenses (Noyes, 2016).

El derecho a la privacidad, entendido como la protección contra los registros e incautaciones irrazonables, está contemplado en la Cuarta Enmienda de la Constitución de Estados Unidos. La cual establece que, si existe consentimiento del titular el registro o incautación será considerado razonable y no se requerirá una orden. Además, obliga a las cortes a considerar la expectativa de privacidad que poseía el individuo para decidir si aplica o no la Cuarta Enmienda, como también a determinar si la expectativa de privacidad es objetivamente razonable (Francis y Francis, 2017).

En 1973, ante el uso creciente de sistemas automatizados de recolección y almacenamiento de datos de carácter personal, tanto en el sector público como el privado, el gobierno de EEUU publicó un reporte titulado Prácticas de Información Justa (*Fair Information Practices*, FIPs), el cual estableció cinco principios básicos para la protección de datos personales (Francis y Francis, 2017):

1) No deben existir sistemas secretos de recolección y almacenamiento de datos personales.

2) Debe existir alguna forma para que un individuo pueda saber qué información poseen de él y para qué la utilizan.

3) Debe existir una forma para que un individuo sea capaz de prevenir que información de él que fue recolectada con un fin, sea utilizada o puesta a disposición para otros usos, sin su consentimiento.

4) Debe existir una forma para que un individuo pueda corregir o enmendar información identificable sobre él.

5) Cualquier organización que crea, mantiene, utiliza o transfiere datos personales identificables, debe asegurar la fiabilidad de su sistema, en cuanto a que los datos sean utilizados para los fines declarados y a las precauciones adoptadas para prevenir el mal uso de los datos.

La principal crítica al FIPs, es que la legitimidad del tratamiento de datos descansa principalmente en uso del sistema "*notice and choice*" (notificación y elección), en el cual se informa al titular sobre las políticas de privacidad y éste debe decidir si las acepta o no (Francis y Francis, 2017). Este sistema, deja la responsabilidad de elección en los individuos y como vimos previamente, los estudios de racionalidad limitada del consumidor y de la paradoja de la privacidad, han demostrado que los individuos toman decisiones irracionales y muchas veces inconsistentes con sus preferencias declaradas. Adicionalmente, Francis y Francis (2017) explican que la mayoría de las personas acepta las políticas de privacidad sin leerlas (textos largos, densos y legalistas), y que, además, la irracionalidad del consumidor está plagada de sesgos, como el que nos lleva a mantener el statu quo y, por ende, aceptar las políticas que nos presentan por default.

Las Prácticas de Información Justas, son una guía de buenas prácticas para las instituciones, públicas y privadas, que recolectan, almacenan y tratan datos personales.

Por ende, son voluntarias. El sector privado en EEUU históricamente se preocupó de evitar regulaciones que pudieran impedir el crecimiento de la economía y comunicación digital, y la primera vez que el Congreso de EEUU promulgó una ley de privacidad (*Privacy Act*, de 1974), inspirada en las FIPs, el fuerte lobby de las compañías de servicios financieros logró que la legislación sólo aplicara a las agencias federales y no a las firmas privadas (The Economist, 2019). Esto significó, que durante muchos años la protección de datos personales se basó en la auto regulación y en la creación de normas específicas para los distintos sectores económicos que pudieran manejar datos más sensibles. Este es el caso del sector de la salud, la educación y las finanzas, que se expone a continuación.

1) HIPAA (*Health Insurance Portability and Accountability Act*), de 1996, que buscó facilitar la transferencia de información médica entre proveedores y pagadores, basándose principalmente en el modelo de "*notice and choice*". Pese a que la privacidad no fue el objetivo principal, el Congreso sí reconoció la necesidad de proteger la privacidad para facilitar esta transferencia (Francis y Francis, 2017).
2) FERPA (*Family Educational Rights and Privacy Act*), de 1974, protege los registros educacionales de los estudiantes que asisten a establecimientos que reciben fondos del gobierno federal, dejando fuera a los establecimientos privados (Francis y Francis, 2017).
3) RFPA (*the Right to Financial Privacy Act*), de 1978, ley que establece derechos y protección sobre la información financiera, en territorio estadounidense, de las personas naturales y de sociedades de cinco o menos individuos, como también de aquellas instituciones u organismos que manejan datos de menores (Francis y Francis, 2017).
4) En 1999, se aprobó el *Gramm-Leach-Biley Act* (GLBA), que modernizó las instituciones financieras e incluyó la obligación de proteger la confidencialidad de la información de sus clientes, mediante la notificación anual de políticas de privacidad y el modelo "*notice and choice*" (Francis y Francis, 2017).

La legislación estadounidense no considera reglas para la transferencia transfronteriza de datos y la preocupación de los distintos gobiernos, desde la llegada de internet, se ha enfocado en mantener el libre flujo de datos. La administración del presidente Bill Clinton, en 1997, reconoció la importancia de proteger el acceso al mercado de los datos y estableció "la primera serie de principios globales relacionados a la gobernanza del flujo transfronterizo de datos –el marco para el comercio electrónico global" (Aaronson y Leblond, 2018, p.10). El objetivo principal, era evitar que las regulaciones nacionales extranjeras se convirtieran en barreras para su comercio digital.

Desde el año 2016, las compañías estadounidenses pueden solicitar su adhesión al *Privacy Shield*, acuerdo entre EEUU y la Unión Europea que permite la transferencia internacional de datos personales, siempre que se establezca que la organización estadounidense en cuestión posee un "nivel adecuado" de protección bajo los estándares europeos. La Comisión Federal del Comercio de EEUU, es el organismo de control y, por ende, el encargado de hacer cumplir el acuerdo. Sin embargo, con la entrada en vigencia del RGPD, la revisión de EEUU como "país adecuado" parece inminente

Estados Unidos ha publicado diversas leyes de protección de datos personales a nivel estatal y federal, que buscan abordar problemáticas sectoriales y muchas veces aplican simultáneamente. El Estado de California es el que posee la legislación más ambiciosa y parecida al RGPD, pero hay otros Estados que ofrecen niveles de protección muy inferiores, creando un campo de juego desnivelado para las compañías (Lehuedé, 2019).

En este escenario, como se planteó en The Economist (2019), los Republicanos y las compañías tecnológicas buscan crear una nueva ley federal, más permisiva que la de California, y que ésta la sobrepase. Mientras que los demócratas, apuntan a que le ley

federal iguale a la de California, estableciendo los más altos estándares de protección a nivel internacional. La Unión Europea está observando el camino regulatorio que tome EEUU y si la legislación no logra estar al nivel de la UE, las compañías estadounidenses se verán fuertemente afectadas por la restricción al flujo de datos desde la UE.

Paralelamente, el gobierno de Donald Trump optó por restarse del Acuerdo Transpacífico (TTP, por sus siglas en inglés), que buscaba "establecer el libre flujo transfronterizo de información por *default*, limitando el proteccionismo digital y estableciendo un piso de privacidad" (Aaronson y Leblond, 2018, p.11). Este acuerdo, al incluir a cerca del 40% de los actuales usuarios de internet, tenía el potencial de fijar las normas internacionales del flujo transfronterizo de datos. Pese a esto, la administración "ha dejado en claro su preocupación creciente por la competencia de China en los sectores impulsados por los datos y su disposición a responder con medidas proteccionistas" (Aaronson y Leblond, 2018, p.12).

El reino de datos de la Unión Europea

La Unión Europea (UE) cuenta con varios competidores globales fuertes en el sector de las telecomunicaciones y de software, pero el desarrollo de firmas centradas en el tratamiento intensivo de datos personales es aún incipiente. "Mientras la Unión Europea (UE) es el mayor exportador de servicios digitales, las firmas estadounidenses controlan cerca del 54% del mercado digital de la UE, comparado con el 46% de las firmas europeas" (Comisión Europea, 2018). De las 30 empresas de internet globales líderes, capitalizadas en el mercado, la UE solo posee una, Spotify (Suecia), y ocupa el puesto 30 a junio de 2019 (Statista, 2019).

La Unión Europea está apostando por desarrollar políticas de comercio locales para construir su reino de datos y el proyecto de un Mercado Único Digital, es su principal

estrategia. A través de ella, buscan eliminar las barreras al flujo transfronterizo de datos, entre los estados miembro, potenciar los recursos, compartir la gobernanza y alcanzar economías de escala y alcance de datos, mientras garantizan la protección de los datos personales de los ciudadanos europeos (Aaronson y Leblond, 2018).

Sin embargo, algunos países de la UE continúan exigiendo la localización de datos, como Francia (sector público debe utilizar servicios de computación en la nube nacionales, exigiendo que el almacenamiento y procesamiento se realice en el país) y Alemania (almacenamiento de datos personales del sector público en el país y algunos datos relativos al sector de telecomunicaciones, con fines de seguridad y persecución legal), lo que es señalado como barreras al comercio internacional por Cory (2017).

Como vimos previamente, la protección de datos personales en la UE es un derecho humano y las firmas solo pueden recolectar y procesar datos bajo condiciones específicas. El consentimiento explícito e informado, es la base de legitimación del uso y tratamiento de datos, y el incumplimiento de la regulación conlleva cuantiosas multas. La regulación actual en esta materia, corresponde al Reglamento General de Protección de Datos (RGPD). Este Reglamento, posee un alcance extraterritorial e implica que su estándar de protección no es negociable. “Debido a que la UE es un mercado mayor, muchos países están adoptando las políticas de protección de datos de la UE o están trabajando para ser considerados “adecuados”” (Aaronson y Leblond, 2018, p.17).

Cory (2017), señala que es ingenuo pensar que el GDPR, que impide la transferencia transfronteriza de datos a países que no son considerados adecuados, pueda efectivamente impedir o controlar las transferencias, puesto que establecer puntos de control con cada país y con cada compañía que busque transferir datos es insostenible.

Capítulo IV:

Protección de Datos Personales en Chile

Estado del Arte

El 28 de agosto de 1999 Chile promulgó la Ley sobre protección de la vida privada, que reguló el "tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares" (Ley Nº 19.628, 1999). De esta forma, se convirtió en el primer país sudamericano en contar con una legislación de este tipo. Sin embargo, su aprobación no estuvo exenta de críticas. Jijena (2010), quien participó como asesor experto en la discusión legislativa, acusó "graves errores de fondo y de estructura, que desde 1999 han impedido su vigencia efectiva" (p. 414). A continuación, revisaremos brevemente sus aspectos más críticos.

La ley establece un marco de protección a los datos personales[7] frente a su tratamiento por terceros y lo permite solo bajo el alero de la ley y/o cuando el titular lo autorice por escrito –luego de ser debidamente informado sobre el propósito de la recolección y tratamiento, y su posible comunicación a terceros. Al mismo tiempo, le otorga protección especial a los datos sensibles[8], los cuales solo podrán ser tratados cuando la ley lo autorice, exista consentimiento del titular o sea necesario para la prestación de servicios de salud a sus titulares. Es importante destacar que el titular puede revocar la autorización, aunque sin efecto retroactivo y a través de una solicitud por escrito.

[7] La legislación chilena define datos personales como "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables" (Ley N° 19.628, Artículo 2°f, 1999).
[8] "Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual" (Ley N° 19.628, Artículo 2° g, 1999).

En ambos casos, los datos solo deben utilizarse para los fines para los cuales fueron recolectados, salvo que provengan de "fuentes accesibles al público" – algo que no queda especificado en la ley. Sin embargo, las personas jurídicas privadas, por medio de la asociación, pueden vulnerar todas las normas de la ley, debido a que se les permite "el tratamiento de datos sin autorización del titular para su uso exclusivo, el de sus asociados y el de las entidades a las que están afiliadas, ya sea con fines estadísticos, de tarificación u otros" (Lever, Yukich y Cruz, 2016, p. 21-22).

Es importante destacar, que con la promulgación de la Ley de Transparencia y Acceso a la Información Pública (Ley N° 20.285, 2008), se atribuye al Consejo para la Transparencia el rol de velar por el adecuado cumplimiento de la ley 19.628, de protección de datos personales, por parte de los órganos de la administración del Estado. Sin embargo, no se le entregan atribuciones claras y tampoco se le otorgo la capacidad de sancionar por incumplimientos. Por ende, su ámbito de influencia es reducido y en la práctica se ha limitado a la protección de datos personales en el marco de las exigencias de transparencia y acceso a la información de la ley.

Otro aspecto relevante de la legislación, es que determina que el Servicio de Registro Civil deberá llevar un registro de los bancos de datos personales en manos de organismos públicos, el cual tendrá un carácter público y deberá informar el fundamento jurídico de la existencia del banco, su finalidad, los tipos de datos que almacena y describir el universo de personas que comprende. Sin embargo, no existe obligación de mantener un registro de banco de datos personales en manos de organismos privados, algo que Jijena (2010) considera una "omisión grave" y que atribuye al hecho de que la ley "fue redactada con la asesoría directa de grupos, gremios y empresas interesadas en asegurar el negocio que constituye el procesamiento de datos personales" (p. 414). El autor va más allá y agrega que "para no encarecer los costos del negocio, dicen las Actas,

se eliminó la obligación de informar una vez al año a los titulares de los datos sobre su procesamiento, con lo cual se permitió el anonimato que hoy cubre el tráfico indiscriminado de información nominativa" (p. 414).

Las personas tienen el derecho de exigir a quien maneje un banco de datos –o que se dedique al tratamiento- información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito de almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos. Este derecho de acceso, o hábeas data, permite a los titulares comprobar la calidad de sus dados, otorgándoles el derecho a exigir que se modifiquen si son erróneos, inexactos, equívocos o incompletos, e incluso, a solicitar su eliminación en caso de que su almacenamiento carezca de fundamento legal o hayan caducado. Sin embargo, la inexistencia de un registro de bancos de datos en el mundo privado, entre otros aspectos normativos, dificulta la fiscalización de estas compañías y la capacidad de exigir el cumplimiento el principio de calidad de los datos (Salas, 2018).

Por un lado, Jijena (2010) explica que "la norma ha transformado al hábeas data en una mera declaración de intenciones, ya que por la vía de excepciones y por establecer como regla general una enorme libertad en materia de procesamiento de datos personales, se permite su "tratamiento" sin autorización de los titulares" (p. 414). Por ejemplo, "el marketing directo está regulado específicamente en las regulaciones de protección al consumidor, con un sistema de *opt-out*: si el individuo expresamente requiere la suspensión de la comunicación comercial" (Salas, 2018, p. 14). Esto implica que el marketing directo no sería constitutivo de consentimiento expreso.

Por el otro, el derecho de acceso se sometió a la competencia de los tribunales y no de un ente administrativo eficaz y especializado. Como explica Salas (2018), esto ha dificultado la protección efectiva de los datos personales debido a que:

> "Para hacer cumplir la ley, aplicar multas y demandar por daños, el titular de los datos necesita interponer acciones directamente ante el tribunal de justicia. En ambos ejemplos, el demandante deberá probar los hechos y el daño, asumiendo todos los costos asociados a las acciones judiciales" (p. 118).

Este mecanismo no produce jurisprudencia vinculante y, por ende, facilita la interpretación de la ley en casos futuros. Además, incentiva a los operadores jurídicos a "recurrir por intermedio del recurso de protección a los tribunales de justicia, invocando la vulneración de un derecho fundamental, normalmente la privacidad" (Lever et al. 2016, p. 22).

De hecho, a julio de 2018, la Corte Suprema había dictado aproximadamente setenta sentencias relativas a infracciones de la ley, desde su entrada en vigencia (Salas, 2018). Sin embargo, como el objetivo es la protección de derechos constitucionales, las cortes –incluso cuando fallan a favor del titular de los datos- "no pueden condenar pago de indemnizaciones de perjuicios ni imponer sanciones" (Salas, 2018, p. 119). Es importante destacar que el derecho a la protección de datos personales, adquiere rango de derecho constitucional el 16 de junio de 2018, con la entrada en vigencia de la Reforma Constitucional (Ley N° 21.096, 2018).

Por otro lado, la ley incorpora el principio de seguridad de los datos, pero no establece estándares mínimos, lo que dificulta determinar si se tomaron o no las medidas necesarias, y, por otro lado, regula la transmisión de datos a terceros, autorizando la transmisión automatizada de datos si se resguardan los derechos de los titulares o, en el

caso de los organismos públicos, su transmisión sea parte de sus funciones (Viollier, 2017). Además, quedan excluidos de esta norma: los datos recolectados de fuentes accesibles al público, de plataformas y aplicaciones digitales y la transferencia transfronteriza de datos.

Esto último, tiene implicancias sobre el potencial desarrollo de la economía digital, como veremos más adelante, y también sobre la tutela del derecho. Jijena (2010) explica que como la normativa chilena es territorial, las empresas internacionales pueden burlar la ley y expone el siguiente ejemplo: "la prohibición de que existan bancos de datos históricos con antecedentes sobre morosidad comercial de más de 7 años puede vulnerarse fácilmente almacenando dicha información –para comercializarla y elaborar mejores perfiles- en un servidor de internet" (p.418), ubicado fuera del territorio chileno.

La asesoría técnica parlamentaria de Roberts (2018), recoge la opinión de 10 expertos sobre los aportes y falencias de la Ley de Protección de la vida privada de las personas (Ley Nº 19.628, 1999) y concluye que:

> "Las falencias más mencionadas pueden agruparse en tres ítems: una conceptualización poco eficiente (como los conceptos de fuente accesible al público, datos sensibles, nuevos escenarios tecnológicos), una falta de herramientas legales (como la Autoridad de control y el catálogo de infracciones) y funciones poco eficientes que, en conjunto, no entregan una protección efectiva de sus datos personales".

Para concluir, podemos resumir los principales y más relevantes defectos de la regulación chilena en protección de datos personales: la inexistencia de una autoridad independiente de control que vele por el cumplimiento de la ley, en el mundo público y privado, y que sea capaz de aplicar sanciones en caso de incumplimiento; la carencia de

regulación de transmisión transfronteriza de datos; y las amplias excepciones para requerir el consentimiento del titular de los datos (por ejemplo, con el sistema de *opt-out* en el marketing directo).

Comercio internacional

Chile posee una amplia red de tratados de libre comercio, 26 acuerdos, que facilitan el acceso a más del 60% de la riqueza global, donde se incluyen las principales potencias de nuestra era: India, China, Unión Europea, Estados Unidos, Japón, Corea del Sur y Brasil. Esto ha significado que el 95% de las exportaciones en Chile se dirigen a países con tratados de libre comercio, siendo China el principal destino con un 27%, seguido por EEUU con un 14% y Japón con un 9% (DIRECON, 2018).

Nuestro país, según DIRECON (2018), ha incorporado "un tratamiento especial respecto de los productos digitales y los contenidos transmitidos electrónicamente, para los cuales se hace permanente la obligación de no aplicar aranceles aduaneros y se asumió el compromiso de no discriminación" (p. 88). Por otro lado, se han incorporado "artículos sobre transferencia transfronteriza de datos por medios electrónicos, libertad de localización de equipos informáticos y cooperación en ciberseguridad" (p. 88).

La DIRECON (2018), en el Anuario de las Exportaciones Chilenas, divide la exportación de servicios entre servicios tradicionales y no tradicionales, puesto que en Chile existen dos registros oficiales: el del Banco Central de Chile (servicios) y el del Servicio Nacional de Aduanas (servicios no tradicionales), los que se analizan por separado por la naturaleza particular de los sectores que cada uno de ellos reporta.

En el Anuario de exportaciones chilenas 2018 (DIRECON, 2018), se analizan los dos registros oficiales previamente mencionados y de acuerdo al Banco Central, las

exportaciones chilenas de la industria de los servicios alcanzaron US$ 10.098 millones, representando el 13% de las exportaciones totales en 2017. Los servicios ligados a "informática e información", representaron un 3% de las exportaciones de servicios totales y anotaron un alza de 4%, alcanzando los US$ 291 millones. Paralelamente, según el Servicio Nacional de Aduanas, las exportaciones de servicios no tradicionales de Chile, aumentaron un 4% en 2017, alcanzando los US$ 1.019 millones. Un 28% de estos servicios, correspondió al sector de las Tecnologías de la Información (TICs)[9].

La DIRECON (2018) expuso que:

> "El 49% de los envíos de TICs se dirigen a América del Norte, seguido de un 42% a América Latina, en tercer lugar, se ubica Europa con un 8% de participación en las ventas del sector al exterior. Asia y África representan menos del 1% de los envíos chilenos del sector. A nivel de países, destacan Estados Unidos -que por sí solo justifica el 49% de los envíos-, Perú (15%), Colombia (9%) y México (6%)" (p.10).

> "En el último año, el servicio TIC más provisto al exterior fue el de "Suministro de sedes para sitios web y correo electrónico" que pasó de exportar US$ 58,6 millones en 2016 a US$ 77,5 en 2017, representando el 27% de los envíos del subsector. También se destacan los servicios de "Apoyo técnico en computación e informática vía remota" y los servicios de "Transmisión internacional de datos" que tuvieron participaciones de 12,3% y 10,4% respectivamente. El sector cuenta además con prestaciones de "asesorías TICs", "diseño de software original",

[9] La OCDE en "Guide to Measuring the information society" (2011), declara que "los productos TIC deben principalmente tener el propósito de cumplir o habilitar la función del procesamiento de la información y la comunicación por medios electrónicos, incluyendo la transmisión y visualización". Es la clasificación internacional vigente de productos TIC e incluye tanto bienes como servicios.

"desarrollo de aplicaciones", "procesamiento de información", "diseño de redes computacionales" y "monitoreo remoto", por nombrar algunos" (p.10).

Chile cuenta con una gran cantidad de centros de datos (*data center*[10]) en su territorio. Como explica Fajardo (2019), las grandes empresas de telecomunicaciones, las compañías tecnológicas a nivel local y las entidades gubernamentales, manejan sus propios *data center* o arriendan el espacio a terceros en territorio nacional, dependiendo de la criticidad de la información. A la vez, Chile tiene en su territorio más de 60 empresas multinacionales que exportan servicios a sus clientes en el mundo, como Google, Telefónica, Amazon Web Services, WIPRO, IBM y Microsoft (InvestChile, 2018). Google invirtió US$300 millones en su *data center* en Chile y Amazon está evaluando si invierte US$1.000 millones en Chile para su *data center* (Fajardo, 2019).

La agencia local de promoción de inversiones extranjeras, InvestChile (2018) "tiene en cartera 62 proyectos de los llamados Servicios Globales, con un potencial de inversión de US$ 1.924 millones. De ellos, US$1.743 millones corresponden a potenciales inversiones en centros de datos" (el 90%). El atractivo de Chile, según Fajardo (2019), radica en diversas razones: (1) estabilidad política, legislativa y financiera; (2) la mejor conectividad en América Latina (le sigue Brasil), con dos cables submarinos de fibra óptica; (3) proyecto fibra óptica austral y nuevo cable submarino entre Chile y Asia; (4) Proyecto de Google ("Curie") para construir cable submarino que comunicaría a Chile con EEUU; (5) conocimientos técnicos; (6) cercanía con grandes mercados, tanto de forma física como en cuanto a relaciones bilaterales.

[10] "Un data center es un centro de procesamiento de datos informáticos que está ubicado en un lugar específico y con una infraestructura adecuada para almacenar, proteger y transmitir la información velozmente a otro lugar mediante redes de banda ancha" (Fajardo, 2019).

La medición de la economía digital en Chile se ha realizado tradicionalmente con foco en el equipamiento tecnológico y de comunicaciones, software, comercio electrónico y niveles de penetración de banda ancha. Bajo este método, y según estudio de Accenture y Oxford Economics (2016), la economía digital representó el 5% del PIB de Chile en 2016. Sin embargo, el estudio asegura que esta medición no incorpora el "valor que aporta la tecnología digital a todos los sectores de la economía a partir del uso de talento, equipos y bienes intermedios digitales empleados en la producción" y propone un nuevo modelo estadístico con el cual la economía digital en Chile habría alcanzado el 22,2% del PIB en 2016, equivalente a 55 mil millones de dólares.

Este mismo estudio, prevé que el 22,2% que aporta la economía digital al PIB de Chile "podría crecer tres puntos porcentuales hasta alcanzar el 25,3% del PIB en el 2021, o 26,3% del PIB para el mismo año, si se optimizasen los impulsores de valor digital". Estos impulsores son: Aceleradores Digitales (ecosistema donde se desarrolla la economía digital), Talento Digital y Tecnologías Digitales. La inversión sub óptima en tecnologías digitales se señala como el mayor obstáculo para crear valor, seguido por la necesidad de aumentar la inversión en aceleradores digitales (acceso al financiamiento, visión digital del gobierno y regulación adecuada, entre otras).

Accenture y Oxford Economics (2016), explican que:

> "En el 2021 el PIB chileno podría alcanzar USD 295 mil millones (escenario optimizado) en vez de USD 282 mil millones (escenario base). En términos de crecimiento, la optimización sumaría un 1% adicional por año, por encima del 2,7% proyectado. He aquí un efecto multiplicador nada despreciable, que elevaría la tasa de crecimiento del país al 3,7% anual".

Por otro lado, el informe de productividad del Ministerio de Hacienda (2017), asociado al proyecto de ley Boletín 11.144-07, aseguró que "mantener la actual regulación implicaría continuar con una normativa insuficiente y obsoleta, que no protege adecuadamente los derechos de la ciudadanía y que podría tener efectos económicos relevantes en la economía" (p.5). De esta forma, no contar con adecuados estándares de protección de datos frenaría -principalmente- el desarrollo de la industria de servicios globales y el de las exportaciones de servicios. Esto a su vez, impactaría negativamente la atracción de inversiones y el desarrollo de innovación tecnológica, junto con el capital humano avanzado.

La expectativa del Ministerio de Hacienda (2017) con el proyecto de ley, era lograr efectos económicos positivos para el país, aumentando las exportaciones de servicios, principalmente en la industria de servicios globales, y la inversión en esos sectores. Para fomentar la instalación de empresas extranjeras de servicios globales en Chile, sería necesario contar con adecuados niveles de protección de datos debido a que en la actualidad "las empresas no tienen garantías suficientes de un manejo lícito de la información privada tratada dentro del país" (p.17), lo que hace que Chile sea menos competitivo a nivel internacional.

El proyecto ley presentado en 2017 (Boletín 11.144-07), según el Ministerio de Hacienda (2017), buscaba cumplir con el compromiso de Chile ante la OCDE (2010), de avanzar en reformas en materia de protección de la privacidad y flujo transfronterizo de datos. Buscando equilibrio entre protección de los derechos y libertades de las personas, con la libre circulación de la información. Esa regulación, seguía los lineamientos de la OCDE en materia de protección de datos personales e incorporaba los principios rectores reconocidos en las directrices OCDE, el modelo europeo y el de

EEUU. Este proyecto de ley (Boletín 11.1444-07), fue refundido con el Boletín 11.092-07, y es este proyecto de ley refundido el que analizaremos a continuación.

Proyecto de ley

Desde de la entrada en vigencia de la Ley N° 19.628 de Protección de la Vida Privada en 1999, se han presentado 67 proyectos de ley sobre datos personales y protección de la vida privada. En 2018, 37 de ellos continuaban en tramitación, 24 fueron archivados y 5 publicados (Biblioteca del Congreso Nacional [BCN], 2018).

En marzo de 2017, el gobierno presentó el proyecto de ley que "Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales" (Proyecto de Ley N° 11.144-07, 2017), que modifica la ley Nº 19.628 sobre protección a la vida privada de forma sustantiva. El proyecto, es refundido con el Boletín 11.092-07 y para realizar el siguiente análisis, utilizaremos el "Texto tentativo de la ley Nº 19.628 sobre protección a la vida privada, si se aprueba el proyecto de ley refundido" (Comisión Constitución, Legislación, Justicia y Reglamento del Senado, 2018).

Objetivo y alcance de la ley

El objetivo de la ley es regular la forma y condiciones en la cual se realiza la el tratamiento y protección de datos personales (de personas naturales), conforme al artículo 19 Nº 4 de la Constitución Política (derecho a la protección de datos personales), mencionada previamente. Su ámbito de aplicación comprende todo tratamiento de datos personales que realicen personas naturales y jurídicas, en el sector público y privado, como también aquellos responsables del tratamiento con residencia en Chile. Se excluye de este régimen el tratamiento de datos personales realizado en el ejercicio de la libertad de opinión e información, como también el que realicen personas naturales con respecto a actividades personales (Proyecto de Ley N° 11.144-07, 2017, Artículo 1).

En el Artículo 2 del Proyecto de Ley (2017), se profundizan una serie de definiciones, dentro de las cuales destacamos las siguientes:

Dato personal: "cualquier información vinculada o referida a una persona natural identificada o identificable", además de indicar que se considerará "identificable, toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante información combinada con otros datos…". De esta forma, se reconoce el potencial del big data.

Dato sensible: "datos personales que revelen el origen étnico o racial, la afiliación política, sindical o gremial, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural". Pasa de una definición amplia incorporando aquellos datos que revelen el origen étnico (además de racial), la afiliación sindical o gremial (además de la política), las convicciones ideológicas o filosóficas, la religión, la salud, el perfil biológico, los datos biométricos, orientación sexual e identidad de género. Es importante destacar que el tratamiento de datos sensibles, solo está permitido cuando existe el consentimiento expreso del titular y plantea algunas excepciones, como cuando está en riesgo la vida del titular o existe una urgencia sanitaria, entre otras (Proyecto de Ley Nº 11144-07, 2017, Artículo 16 y 16 bis).

Es importante destacar que los datos personales relativos a menores de edad, también cuentan con una protección especial y solo pueden ser tratados "atendiendo el interés superior de éstos y al respeto de su autonomía progresiva" (Proyecto de Ley Nº 11144-07, 2017, Artículo 16 quinquies). Para esto, se requiere el consentimiento de los padres o representantes legales o mandato de ley. Los establecimientos educaciones,

como también las entidades públicas o privadas que traten o administren datos personales de menores de edad, están obligados a velar por el uso lícito y la protección de la información personal en su poder.

Fuentes de acceso público: "todas aquellas bases de datos o conjuntos de datos personales, públicos o privados, cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, siempre que no existan restricciones o impedimentos legales para su acceso o utilización" (Proyecto de Ley Nº 11144-07, 2017, Artículo 2). Es importante destacar que el Presidente de la República presentó indicaciones sobre este ítem (Indicaciones del Ejecutivo, 2019) señalando que será el Consejo para la Transparencia y la Protección de los Datos Personales, quien "deberá establecer de forma taxativa las bases de datos que cumplan esta categoría", y revisarla anualmente.

Responsable de datos o responsable: "toda persona natural o jurídica, pública o privada, que decide acerca de los fines y medios del tratamiento de datos personales, con independencia de si los datos son tratados directamente por ella o a través de un tercero mandatario o encargado". (Proyecto de Ley Nº 11144-07, 2017, Artículo 2). El tercero mandatario o encargado, se considera responsable solo cuando trata, cede o entrega datos con un objeto distinto al acordado con el mandante (responsable). Quienes "presten servicios de infraestructura, plataforma, software u otros servicios para el almacenamiento o procesamiento de los datos, o para facilitar enlaces o instrumentos de búsqueda, no tendrán la calidad de responsable de datos", siempre que no tomen decisiones sobre los medios y fines del tratamiento (Proyecto de Ley Nº 11144-07, 2017, Artículo 15 bis).

Titular de datos o titular: “persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales” (Proyecto de Ley Nº 11144-07, 2017, Artículo 2).

Consentimiento: “toda manifestación de voluntad libre, específica, inequívoca e informada” (Proyecto de Ley Nº 11144-07, 2017, Artículo 2), donde el titular de los datos o su representante legal, autoriza el tratamiento de sus datos.

Principios

Como se evidenció en capítulos anteriores, las regulaciones que buscan proteger los datos personales pueden generar efectos económicos y los principios que rigen el tratamiento, marcan fuertemente las reglas del juego y tienen el potencial de limitar o impulsar el desarrollo económico. A continuación, revisaremos los principios del Proyecto de ley (Proyecto de Ley Nº 11144-07, 2017, Artículo 3), y su potencial efecto económico.

(a) Principio de licitud del tratamiento: el tratamiento se debe realizar con sujeción a la ley.

(b) Principio de finalidad: la recolección de datos debe realizarse con fines específicos, explícitos y lícitos, y su tratamiento de deberá limitar al cumplimiento de éstos. Se permitirá el tratamiento de datos con fines distintos a los autorizados, siempre que: éstos sean compatibles con el fin original; exista una relación contractual o pre contractual entre los involucrados que justifique el tratamiento; los datos provengan de fuentes accesibles al público; o lo disponga la ley. Al igual que el RGPD, un nuevo tratamiento requerirá que el titular de los datos otorgue nuevamente su consentimiento.

(c) Principio de proporcionalidad: el tratamiento de datos debe limitarse a los fines declarados. Esto implica que no se pueden recolectar datos de forma excesiva y que los datos, solo se podrán almacenar por el tiempo necesario para la finalidad declarada,

momento en el cual se requeriría un nuevo consentimiento del titular o la cancelación o anonimización de los datos.

(d) Principio de calidad: indica que los datos deben ser exactos, completos y actuales, con respecto a los fines del tratamiento.

(e) Principio de responsabilidad: establece que quienes realicen el tratamiento de los datos personales serán responsables legalmente del cumplimiento de la ley.

(f) Principio de seguridad: obliga al responsable del tratamiento a garantizar estándares adecuados de protección, mediante acciones técnicas u organizativas adecuadas. Solo ante un incidente de seguridad, y cuando exista una controversia judicial o administrativa, el responsable deberá acreditar la existencia de las medidas de seguridad adoptadas. El responsable deberá reportar las vulneraciones a la seguridad de los datos al organismo de control siempre y en el caso de los titulares afectados, solo cuando se trate de datos sensibles o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, o cuando exista un riesgo razonable de que la vulneración genere prejuicios o afectación al titular.

(g) Principio de transparencia e información: exige que las políticas y prácticas sobre el tratamiento de los datos personales, sean claras, precisas e inequívocas, y que estén siempre accesibles y a disposición del público de forma gratuita. Se obliga al responsable del tratamiento a adoptar todas las medidas necesarias para facilitar el acceso del titular a esta información.

(h) Principio de confidencialidad: recae sobre el responsable de datos personales y las personas que tienen acceso a ellos, estableciendo la obligación de implementar controles y medidas para resguardar el secreto o confidencialidad. A diferencia del GDPR, no obliga a demostrar ex antes que las tomó.

Los principios del Proyecto de ley van en línea con los principios del RGPD, pero presentan algunas diferencias que podrían tener implicancias económicas, como observaremos a continuación.

El RGPD posee el principio de *accountability* (rendición de cuentas), el cual obliga al responsable del tratamiento o procesamiento a tener la capacidad de demostrar que cumple con sus obligaciones. Esto implica que todos los principios deben ser demostrados ex antes, a diferencia del principio de seguridad y confidencialidad del proyecto chileno, donde se debe acreditar su cumplimiento solo ante una vulneración de ellos (ex post). A la vez, ante la ocurrencia de vulneraciones a las medidas de seguridad adoptadas, el RGPD es más exigente y obliga a informar al titular afecta siempre, mientras que el proyecto chileno considera esta comunicación solo cuando se trate de datos personales con protección especial (como datos sensibles o bancarios) o exista un riesgo razonable de afectación al titular. La mayor exigencia del RGPD aumenta el costo del tratamiento de datos y el riesgo asociado a ello, en mayor medida que el proyecto de Chile.

Por otro lado, el RGPD incluye en el principio de transparencia que el tratamiento sea "justo" y el principio de integridad y confidencialidad obliga al responsable a contar con un Oficial de Datos Personales, quien estará a cargo de velar por el cumplimiento legal del tratamiento. Estos dos aspectos no son parte de los principios del proyecto de ley en Chile. La obligación de contar con un Oficial de Datos Personales aumenta el costo del tratamiento y la exigencia de que el tratamiento sea "justo", limita la capacidad de utilizar los datos, por lo que podríamos pensar que el proyecto chileno, en este aspecto, podría afectar en menor medida el potencial económico de los datos.

Otra diferencia importante se da entre las fuentes de licitud del tratamiento de datos personales del RGPD y el proyecto de ley chileno. El proyecto chileno considera

que los datos personales obtenidos de “fuentes de acceso público” no requerirán del consentimiento del titular para su tratamiento, algo que no existe en el RGPD. Esto aumentaría el espectro de datos personales que pueden ser tratados legítimamente por un responsable, en comparación al RGPD, por lo que podría permitir desarrollar en mayor medida la innovación y valorización de los datos. Recordemos que el principio finalidad (que limita el tratamiento de los datos para los fines que fueron recolectados), podría impactar negativamente la innovación y el desarrollo económico, puesto que tiene el potencial de aumentar el costo del tratamiento de datos, al limitar las formas en que una empresa o institución puede utilizarlos una vez que los recolectó.

Las obligaciones legales que recaen en el responsable del tratamiento de datos, a raíz de los principios que establece el proyecto de ley, tienen el potencial de aumentar el riesgo de realizar el tratamiento de datos y su costo. Pese a que el proyecto de ley chileno es menos exigente que el RGPD, su efecto económico podría ser importante.

Derechos del titular

El proyecto de ley contempla una serie de derechos de los titulares de los datos, conocidos como derechos ARCOP: acceso, rectificación, cancelación, oposición y portabilidad. Estos derechos son personales, intransferibles e irrenunciables, no pudiendo limitarse por ningún acto o convención. En caso de muerte del titular, sus derechos podrán ser ejercidos por sus herederos (Proyecto de Ley Nº 11144-07, 2017, Artículo 4). Los derechos ARCOP son parte del RGPD.

- **Derecho de Acceso**: permite al titular solicitar y obtener información del responsable, sobre el tratamiento de sus datos personales. Qué datos se están tratando, cuál es su origen, cuál es la finalidad o finalidades del tratamiento, a quién se han comunicado o cedido los datos (o se prevé hacerlo) y cuánto tiempo durará el tratamiento. El responsable podrá no entregar la información solicitada

cuando “su comunicación resulte imposible o su entrega exija un esfuerzo desproporcionado”, cuando imposibilite u obstaculice el tratamiento de datos con fines de interés público (históricos, estadísticos, científicos) o que vayan en beneficio de la salud humana, o cuando lo disponga expresamente la ley (Proyecto de Ley Nº 11144-07, 2017, Artículo 5).

- **Derecho de rectificación**: el titular puede solicitar al responsable del tratamiento la rectificación de sus datos personales, cuando éstos sean inexactos, desactualizados o incompletos (Proyecto de Ley Nº 11144-07, 2017, Artículo 6).
- **Derecho de cancelación**: del titular a solicitar y obtener del responsable la supresión o eliminación de sus datos personales, cuando estos no sean necesarios para el fin declarado de tratamiento, el titular haya revocado su consentimiento, hayan sido tratados ilícitamente, sean datos caducos o el titular haya ejercido su derecho de oposición, entre otros. Este derecho tiene también algunas limitantes, como cuando existen razones de interés público (especialmente en temas de salud) (Proyecto de Ley Nº 11144-07, 2017, Artículo 7).
- **Derecho de oposición**: establece que el titular podrá oponerse al tratamiento de sus datos ante el responsable cuando: afecte sus derechos y libertades fundamentales; el tratamiento tenga como fin exclusivo acciones de marketing directo; falleció el titular de los datos (herederos ejercen el derecho); y cuando el tratamiento se realice en base a datos obtenidos de fuentes de acceso público y no exista otro fundamento legal para su tratamiento (Proyecto de Ley Nº 11144-07, 2017, Artículo 8).
- **Derecho de oposición a valoraciones personales automatizadas**: Al igual que el RGPD, el proyecto de ley consigna el derecho a no ser sujeto de decisiones que lo afecten y que estuvieron basadas exclusivamente en el tratamiento

automatizado de sus datos personales (incluyendo la elaboración de perfiles), aunque a diferencia del RGPD, estas decisiones deben afectarlo "significativamente en forma negativa o le produzcan efectos jurídicos adversos" (Proyecto de Ley Nº 11144-07, 2017, artículo 8º bis), para poder ejercer este derecho. De todas formas, el titular podrá exigir intervención humana y solicitar la revisión de la decisión cuando corresponda de acuerdo a la ley.

- **Derecho a la portabilidad de los datos personales**: permite al titular solicitar y obtener del responsable una copia de sus datos personales "de manera estructurada, en un formato genérico y de uso común, que permita ser operado por distintos sistemas". Este derecho, no incluye aquella "información que haya sido inferida, derivada, creada, generada u obtenida a partir del análisis o tratamientos realizados por el responsable". Tampoco cuando sea un "volumen relevante de datos y sean tratados de forma automatizada" o sea necesario para la celebración de un contrato.

El derecho de rectificación, cancelación y oposición serán gratuitos para el titular, al igual que el derecho de acceso (trimestralmente). El responsable de datos podrá exigir el pago de los costos directos en que incurra cuando el titular solicite la portabilidad de sus datos. Es importante desatacar, que cuando se formula una solicitud de rectificación, cancelación u oposición, el titular tiene el derecho a solicitar y obtener del responsable el bloqueo temporal de sus datos o del tratamiento de éstos. El responsable tendrá dos días para responder dicha solicitud, periodo en el cual no podrá tratar los datos en cuestión.

Estos derechos tienen el potencial de generar dos efectos económicos. El primero y más básico, es el aumento del costo del tratamiento de datos personales. El responsable debe contar con un sistema y/o capital humano para permitir que los titulares puedan ejercer sus derechos. El segundo, tiene que ver con el efecto del ejercicio de estos

derechos sobre el valor de los datos y sobre los sistemas que se alimentan de los datos, como la inteligencia artificial. Cuando solicitan el derecho de cancelación o revocan el consentimiento para el tratamiento, el responsable ya ha realizado una inversión para el tratamiento y estimado sus costos, asignándole un valor a los datos. Cuando estos derechos son ejercidos, el valor del dato puede cambiar e incluso podría pasar a ser negativo. A la vez, si el dato en cuestión formaba parte de un sistema de inteligencia artificial y debe ser eliminado, podría comprometer el sistema por completo y, por ende, afectar su valor.

A diferencia del RGPD, la rectificación, cancelación u oposición al tratamiento de datos en el proyecto de ley chileno, se aplicaría solo al responsable a quien se le formuló la solicitud. Sería deber de este, comunicar a quienes les haya cedido o comunicado dichos datos, pero queda la duda de si éstos deberán cumplir con la solicitud del titular. Esto podría ser positivo desde el punto de vista económico, porque si el responsable vendió los datos a un tercero a un valor y posteriormente le solicita eliminarlos, ese valor podría pasar de ser positivo a negativo.

El derecho a la portabilidad podría tener efectos económicos positivos y negativos. Por un lado, puede aumentar el costo para el responsable y reducir el valor de los datos que tiene en su poder, afectándolo negativamente. Por el otro, podría ayudar a disminuir las barreras de entrada para nuevos competidores en el mercado de los datos, promoviendo la innovación y la competencia del mercado. Sin embargo, aún está por verse la factibilidad técnica real de ejercer este derecho.

Licitud del tratamiento

La regla general es que el tratamiento de datos personales será lícito, cuando el titular otorgue su consentimiento para ello. El consentimiento debe ser “libre, informado y específico en cuanto a su finalidad o finalidades”, y debe manifestarse de forma

inequívoca, ya sea con una declaración verbal, escrita o por medios electrónicos (Proyecto de Ley Nº 11144-07, 2017, Artículo 12).

El titular tiene el derecho de revocar el consentimiento en cualquier momento y sin expresión de causa, pero sin efectos retroactivos. Esto buscaría proteger el buen funcionamiento de los sistemas que se alimentan y crecen a partir de los datos, como la inteligencia artificial. Sin embargo, no queda claro qué sucedería cuando el responsable del tratamiento cede los datos un tercero y si éste último puede o no continuar con el tratamiento de estos. Al igual que el RGPD, el solo consentimiento no es suficiente para que el tratamiento sea lícito, puesto que si existe un "desequilibrio ostensible entre la posición del titular y el responsable" el consentimiento no se considerará una base jurídica suficiente. Esto protegería a los titulares de los datos ante la asimetría de poder que abordamos en el Capítulo I.

El proyecto de ley, también considera otras fuentes de licitud del tratamiento en el Artículo 13, estableciendo que el tratamiento será lícito cuando: los datos provengan de fuentes de acceso público y su tratamiento se relacione con el fin para el cual fue recolectado; sea necesario para cumplir obligaciones legales o lo disponga la ley; sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable; sea necesario para formular, ejercer o defender un derecho ante tribunales; y cuando sea necesario para "la satisfacción de intereses legítimos del responsable o de un tercero, siempre que con ello no se afecten los derechos y libertades del titular". La principal diferencia aquí con el RGPD es la inclusión del concepto "fuentes de acceso público" y el proyecto de ley establece que la autoridad de control deberá establecer de forma taxativa, anualmente, las bases de datos que caigan en esta categoría. Quedará por verse la factibilidad técnica y real de esta medida, puesto que el aumento explosivo de datos

personales seguirá creciendo y probablemente, la revisión anual de la categoría resulte insuficiente. Por otro lado, deja espacio para la discrecionalidad administrativa.

Tratamiento de datos personales por los órganos públicos

El proyecto de ley diferencia el tratamiento de datos que puede realizar el sector público y el privado, estableciendo que las instituciones públicas no necesitarán del consentimiento del titular cuando el tratamiento que realicen se enmarque en el cumplimiento de sus funciones legales y esté dentro del ámbito de sus competencias, de conformidad a las normas establecidas en la ley (Proyecto de Ley Nº 11144-07, 2017, Artículo 20).

A los principios que deben regir todo tratamiento de datos (contenidos en el Artículo 3 del proyecto), a los órganos públicos se le agregan los principios de eficiencia, transparencia, publicidad y coordinación (Proyecto de Ley Nº 11144-07, 2017, Artículo 21). El principio de coordinación implica alcanzar un alto grado de interoperabilidad y coherencia entre las instituciones. Para cumplir con el principio de eficiencia, se deberá evitar la duplicación de procedimientos y trámites entre los organismos públicos y entre éstos y los titulares de los datos. Frente al principio de transparencia y publicidad, los organismos públicos deberán dar acceso a la información en su poder, con el debido resguardo de las funciones fiscalizadoras e inspectoras y los derechos de las personas.

Mientras que los principios que deben regir el tratamiento de datos en los órganos públicos se amplían los derechos de los titulares se reducen. El proyecto de ley indica que no sería aplicable a los órganos públicos lo señalado en el Artículo 10, que habla del deber del responsable de implementar mecanismos que permitan al titular ejercer sus derechos en forma expedita, ágil y eficaz. Además, no permite ejercer el derecho de oposición a valoraciones personales automatizadas (Proyecto de Ley Nº 11144-07, 2017, Artículo 8 bis) y el derecho a la portabilidad de los datos personales (Proyecto de Ley Nº 11144-07,

2017, Artículo 9). Por otro lado, sí se reconoce el derecho de acceso, rectificación y oposición, mientras que el derecho de cancelación solo podrá ejercerse cuando el tiempo necesario para cumplir con la finalidad de la recolección haya finalizado (Proyecto de Ley Nº 11144-07, 2017, Artículo 23).

La cesión o comunicación de datos personales entre organismos públicos estaría permitida, siempre que se enmarque dentro de sus funciones, y solo requerirá del consentimiento del titular si se dirige a una persona o institución privada (cuando no se trate de labores de propias de fiscalización o inspección) (Proyecto de Ley Nº 11144-07, 2017, Artículo 22). Las condiciones bajo las cuales se podrán realizar estas acciones (cesión o comunicación), serán determinadas por un reglamento expedido por el Ministerio Secretaría General de la Presidencia y suscrito por el Ministerio de Hacienda, previo informe del organismo de control. También se regulará de esta forma, los procedimientos de anonimización de los datos personales y datos sensibles (Proyecto de Ley Nº 11144-07, 2017, Artículo 26). (Este reglamento no se aplicará a los órganos públicos del título VIII de esta ley (Congreso, Poder Judicial y organismos autónomos constitucionales)).

Los organismos públicos quedan excluidos del deber de reportar a la autoridad de control las vulneraciones a las medidas de seguridad que implique un riesgo para los derechos y libertades de los titulares y el deber de informar a los titulares de los datos, cuando la vulneración afecte datos sensibles, de menores de 14 años o relativos a obligaciones comerciales, financieras, económicas o bancarias (Proyecto de Ley Nº 11144-07, 2017, Artículo 14 sexies).

Organismos autónomos constitucionales

Corresponderá a los órganos internos de estas instituciones ejercer las funciones que la ley encomienda a la autoridad de control. Las autoridades de estos organismos

deberán dictar las políticas, normas e instrucciones necesarias para cumplir con los principios y obligaciones de la ley, pudiendo requerir para ello la asistencia técnica de la autoridad de control.

Estas instituciones, como norma general deberán cumplir con lo que señala el Título IV: Del tratamiento de datos personales por los órganos públicos, que explicamos con anterioridad, y que excluye varios artículos que aplican para el mundo privado. Sin embargo, a las excepciones a la ley que ya se contemplan para los órganos públicos, se le agrega la excepción de la aplicación del Artículo 14° quinquies, el cual se refiere al deber del responsable de adoptar medidas de seguridad tendientes a resguardar el cumplimiento del principio de seguridad que establece la ley, además de obligar al responsable a acreditar la existencia y funcionamiento de estas medidas ante la ocurrencia de un incidente de seguridad.

Cuando un titular sienta que se han vulnerado sus derechos o se han incumplido los principios que deben regir el tratamiento de sus datos personales, en el Congreso, Poder Judicial u órganos con autonomía constitucional, podrán reclamar ante la Corte de Apelaciones (Proyecto de Ley Nº 11144-07, 2017, Artículo 58).

La autonomía que se exige a los organismos de control, a nivel internacional, no se garantiza en el caso de estas instituciones, donde los datos personales que están en su poder quedan a merced de juez y parte, y, además, con menores garantías que en el resto de los organismos públicos y el sector privado**.** Como el Poder Judicial debe decidir sobre las decisiones que toma la autoridad de control en materia de protección de datos personales, es razonable que quede fuera de su vigilancia. Sin embargo, la exclusión del Congreso y los organismos con autonomía constitucional no se justifica.

Con estas excepciones, la protección de los datos personales en manos de organismos públicos entrega menos garantías a los titulares que el sector privado y aún

más vulnerable, es la situación de los datos personales en los órganos públicos que señala el título VIII de este proyecto ley (Congreso, Poder Judicial y organismos con autonomía constitucional).

Transferencia internacional de datos personales

Como regla general, y siempre que exista licitud en el tratamiento de datos, se permitirá la transferencia internacional de datos cuando: la transferencia se realice a una persona, entidad u organización sujeta al ordenamiento jurídico de un país con un nivel de protección adecuado; cuando existan cláusulas contractuales u otros instrumentos jurídicos, que establezcan derechos y garantías de titulares, y obligaciones de los responsables, además de medidas de control; cuando exista un modelo de cumplimiento o autorregulación vinculante y certificado entre quien transfiere y quien recibe; cuando exista consentimiento expreso del titular; cuando se refiera a transferencias bancarias; cuando se realice entre sociedades o entidades de un mismo grupo empresarial, o empresas relacionadas sujetas a un mismo controlador (con las mismas políticas de protección de datos personales); cuando sea necesario para cumplir obligaciones relativas a convenios o acuerdos internacionales; ejecución de un contrato; emergencias sanitarias (Proyecto de Ley Nº 11144-07, 2017, Artículo 27).

El Artículo 28 (Proyecto de Ley Nº 11144-07, 2017), establece que un país será considerado adecuado, cuando cumpla con estándares similares o superiores a los de esta ley y que será la autoridad de control, la que determinará fundadamente qué países son adecuados. Al menos deberá contar con: principios, normas que garanticen los derechos de los titulares de los datos, autoridad pública jurisdiccional o administrativa de control o tutela (no necesariamente independiente, como el RGPD), obligación de información y seguridad de los responsables, determinación de responsabilidades ante infracciones.

Autoridad de control

En el Proyecto de Ley Nº 11144-07 (2017, Artículo 30), se señala la creación de la Agencia de Protección de Datos Personales, organismo público autónomo, descentralizado, de carácter técnico, con personalidad jurídica y patrimonio propio, "sometido a la supervigilancia del Presidente de la República a través del Ministerio de Hacienda". La autonomía es requisito esencial para ser considerado país adecuado por la Unión Europea y este último párrafo claramente hace que pierda autonomía. El Presidente de la República, Sebastián Piñera, corrigió esta situación en las indicaciones presentadas el 14 de 10 de 2019, señalando que será el Consejo para la Transparencia, el organismo de control de esta ley. Con el Proyecto de ley, pasaría a llamarse Consejo para la Transparencia y la Protección de Datos Personales (CPLTPDP), ampliando su ámbito de acción hacia el sector privado, en relación a la protección de datos personales, e incorporando facultades fiscalizadoras y sancionadoras sobre la materia. Sin embargo, en el sector público se mantiene la limitación de su competencia al Poder Ejecutivo del Estado. De esta forma, el Congreso Nacional, el Poder Judicial y los organismos públicos dotados de autonomía constitucional, serán juez y parte con respecto al tratamiento de datos personales que realicen, como explicamos previamente.

Corresponderá al CPLTPDP aplicar e interpretar administrativamente las disposiciones legales y reglamentarias, vigilando su cumplimiento e impartiendo las instrucciones de carácter general necesarias para el cumplimiento de la ley (Proyecto de Ley Nº 11144-07, 2017, Artículo 31). Fiscalizará y velará por el cumplimiento de principios, derechos y obligaciones en materia de protección de datos personales, y estará facultado para solicitar antecedentes o documentos con este fin. A la vez, resolverá solicitudes y reclamaciones de los titulares en contra de los responsables, investigará y determinará infracciones de los responsables y establecerá sanciones, entre otras funciones.

Las infracciones a la ley pueden ser leves (multas de 1 a 100 UTM), graves (multas de 101 a 1.000 UTM) o gravísimas (multas de 1.001 a 10.000 UTM o en caso de una empresa no regida por la ley N° 20.416, con multa de 1.001 UTM a un monto equivalente al 8% de las utilidades anuales del ejercicio anterior). El RGPD establece multas como un porcentaje sobre las ganancias con un tope, reconociendo las diferencias que pueden existir en el tamaño de las empresas responsables, donde una gran empresa la multa de 10 mil UTM puede ser irrisoria, pero para una pequeña puede significar la quiebra.

Lo que sí hace el proyecto de ley es establecer una serie de circunstancias atenuantes y agravantes (Proyecto de Ley Nº 11144-07, 2017, Artículo 40). Sobre estas, el Consejo deberá considerar la capacidad económica del infractor (cuando es privado), el perjuicio producido (N° de titulares afectados), los beneficios obtenidos por el responsable y el tipo de datos en cuestión (los datos sensibles y de menores de edad se considerarán más graves). Todas las sanciones (de leves a gravísimas) serán registradas en el Registro Nacional de Cumplimiento y Sanciones (anotaciones gratuitas y de acceso público), manejado por el CPLTPDP, por un periodo de 5 años (desde su registro) (Proyecto de Ley Nº 11144-07, 2017, Artículo 43). Las resoluciones del CPLTPDP podrán ser impugnadas ante la Corte de Apelaciones mediante un reclamo de ilegalidad.

Al comparar las categorías de infracciones del proyecto de ley refundido con el RGPD podemos observar que consistentemente la legislación chilena cataloga como grave, situaciones que el RGPD considera gravísimas. El tratamiento sin consentimiento o sin un antecedente o fundamento legal que otorgue licitud a este, o tratarlos con una finalidad distinta a la declarada en la recolección es grave. Comunicar o ceder sin consentimiento, en los casos en que sea necesario el consentimiento, es grave, al igual que comunicar y/o ceder para un fin distinto al autorizado (el RGPD considera esto

gravísimo, por violar el principio de finalidad). Tratamientos innecesarios para el fin, o con datos inexactos, incompletos o desactualizados, para los fines, grave (RGPD lo considera gravísimo porque viola el principio de calidad). Impedir u obstaculizar derechos de acceso, rectificación, cancelación, oposición o portabilidad, grave (RGPD es gravísimo). Omitir respuesta, responder tarde o denegar la petición sin justificación, en los casos de solicitudes fundadas de bloqueo temporal del tratamiento de datos de un titular en grave (RGPD es gravísimo). Tratamiento de datos personales de menores con infracción a normas legales (RGPD es gravísimo). Omitir comunicaciones o los registros en los casos de vulneración de las medidas de seguridad. Vulnerar deber de secreto u obligaciones de seguridad. Seguridad insuficiente. Transferencia internacional en contra de las normas legales es grave (RGPD gravísimo).

El proyecto de ley solo considera como falta gravísima: el tratamiento fraudulento; destinar maliciosamente los datos a una finalidad distinta a la consentida o autorizada por ley; comunicar, transmitir o ceder información no veraz, incompleta, inexacta o desactualizada del titular; vulnerar secreto o deber de confidencialidad sobre datos sensibles o infracciones penales, civiles, administrativas y disciplinarias; comunicar, tratar o ceder datos de menores en contra de la ley; omitir deliberadamente la comunicación de vulneraciones a las medidas de seguridad; realizar a sabiendas transferencias internacionales contrarias a la ley; incumplir resolución del Consejo ante reclamación de derechos de titulares (acceso, rectificación, cancelación, oposición, portabilidad o bloqueo temporal); y entregar información falsa, incompleta o errónea en el proceso de registro o certificación del modelo de prevención de infracciones.

Conclusión

El desarrollo económico de los países dependerá de su capacidad de recolectar, almacenar y tratar datos personales a gran escala. Estamos frente a un nuevo tipo de economía, la economía guiada por los datos, la cual se orienta a los servicios, no reconoce fronteras y presenta grandes fallas de mercado. Es una economía imperfecta, con altos niveles de opacidad, grandes asimetrías de información y de poder, y una fuerte tendencia a la concentración.

Las empresas centradas en el tratamiento masivo de datos personales, que han alcanzado una posición dominante en el mercado, se benefician del efecto red de datos y, por ende, tienen fuertes incentivos para establecer políticas de privacidad que aseguren esa posición. A nivel internacional, los países hacen los mismo. EEUU y China hoy se posicionan como líderes indiscutibles, y buscan regulaciones internacionales que protejan su posición dominante. La Unión Europea intenta entrar en la competencia imponiendo una regulación de protección de datos con alcance extraterritorial, que busca nivelar la cancha para que las compañías europeas puedan competir con los gigantes tecnológicos de las dos potencias.

La regulación de protección de datos personales busca hacer frente a las fallas de mercado inherentes a la economía guiada por los datos. La concentración de los mercados tiene el potencial de reducir los niveles de privacidad ofrecidos y la libertad de elección de las personas, que se pueden ver enfrentados a una situación de "tómalo o déjalo" (asimetría de poder). También hay que considerar que es un mercado donde existen fuertes asimetrías de información, con respecto al uso que se les da a los datos. Las políticas de privacidad son extensas, están escritas en un lenguaje técnico y los verdaderos alcances del consentimiento son difíciles de cuantificar. La empresa tiene claridad de qué

es lo que hará con los datos, la persona que los entrega… difícilmente. Es un mercado opaco, que se beneficia de la racionalidad limitada del consumidor y de la paradoja de la privacidad, donde la valoración de privacidad que declaran tener las personas no siempre se condice con su comportamiento.

Todas las regulaciones que buscan la protección de los datos personales tienen el potencial de generar efectos económicos. "Una protección insuficiente puede generar efectos negativos en el mercado, al reducir la confianza de los consumidores, y una protección excesiva, puede restringir el desarrollo de negocios" (UNCTAD, 2016, p. xii). Debido al carácter global de la economía guiada por los datos, las regulaciones que adopten los diferentes países, desde el aspecto económico, deberían apuntar a: fortalecer la competencia del mercado, asegurar el libre flujo transfronterizo de datos y proveer de certeza jurídica a las empresas que recolectan, almacenan y tratan datos personales.

La regulación de protección de datos personales en Chile está obsoleta y representa un freno para el desarrollo del mercado de servicios globales y la exportación de servicios tradicionales y no tradicionales, reduciendo la competitividad del país a nivel internacional.

Chile es una economía productora. Según el Banco Central, el área de servicios representó solo un 13% de las exportaciones totales en 2017 y de estas, solo un 3% correspondió a servicios de informática y de información (DIRECON, 2018). Al observar las cifras del Servicio Nacional de Aduanas sobre la exportación de servicios no tradicionales, vemos que un 28% correspondió servicios asociados a las Tecnologías de la Información y las Comunicaciones (TICs), y que la exportación de estos servicios se dirigió principalmente Estados Unidos (49%) y América Latina (42%), dejando a la Unión Europea en tercer lugar con un 8% (DIRECON, 2018). Estos servicios utilizan y/o

poseen datos personales y, por ende, para poder desarrollarse necesitan del libre flujo transfronterizo de datos. Finalmente, existen más de 60 multinacionales exportando servicios desde Chile y contamos con una cartera de proyectos de servicios globales que alcanza los US$ 1.924 millones, donde el 90% de los proyectos corresponderían a centros de datos (InvestChile, 2018).

Estas cifras nos demuestran dos cosas: 1) el aporte a la economía de la exportación de servicios globales y TICs en Chile es bajo y, por ende, tiene gran potencial de crecimiento. 2) El principal destino de exportación de estos servicios es Estados Unidos y no la Unión Europea, por lo que garantizar el libre flujo de datos personales con EEUU hoy podría ser más relevante que garantizar el libre flujo con la UE.

El proyecto de ley que actualiza la regulación de protección de datos personales en Chile, busca cumplir con las directrices de la OCDE y sigue los lineamientos del RGPD de la Unión Europea, pensando en que será éste el estándar internacional de protección de datos personales. Actualizar la regulación, que data de 1999, pondría fin a la incerteza jurídica que enfrentan hoy las empresas que manejan datos personales en nuestro país y, por ende, podría impulsar el desarrollo, la innovación y la inversión en el mercado de los datos personales en Chile.

Sin embargo, los principios, derechos y deberes que establece el proyecto de ley, tienen el potencial de aumentar el costo general de la recolección, almacenamiento y tratamiento de datos personales. Porque para cumplir con la nueva regulación, las compañías probablemente invertirán en tecnología y capital humano, como también en seguros que ayuden a enfrentar el aumento del riesgo asociado a la actividad (por las fuertes sanciones económicas por incumplimiento).

La regulación limita lo que se puede hacer con los datos y, por ende, podría disminuir su potencial económico y valor. El principio de finalidad, exige un nuevo consentimiento cada vez que se busque un nuevo objetivo de tratamiento, lo que podría disminuir el valor de los datos recolectados, aumentar el costo de tratamiento y desincentivar la innovación.

El derecho a la portabilidad de los datos puede generar efectos económicos positivos y negativos. Por un lado, podría disminuir las barreras de entrada para nuevos competidores (contrarrestando el poder del efecto red de datos) y favorecer la competencia. Por el otro, podría cambia el valor de los datos que ya fueron recolectados. Sin embargo, aún está por verse la factibilidad real de la portabilidad (técnica y económica).

El derecho de cancelación y a retirar el consentimiento en cualquier momento, tiene el potencial de cambiar el valor de los datos y afectar los sistemas que se alimentan de dichos datos, como la inteligencia artificial y el Internet de las Cosas. El derecho a oponerse a decisiones basadas únicamente en procesos automatizados, podría aumentar el costo de la tecnología y desincentivar su uso e inversión en ella.

La transferencia internacional de datos personales se regulada y contempla diversos mecanismos para permitirla. Los requisitos para considerar un país como “adecuado”, son más laxos que el RGPD (no se exige autonomía del organismo de control, por ejemplo), y permitirían transferir datos con EEUU en un marco de protección. Por otro lado, la regulación fue pensada para lograr que la Unión Europea declare a Chile como “país adecuado” y, por ende, debiera asegurar el libre flujo de datos con ella.

En general, el proyecto de ley de protección de datos personales en Chile podría generar efectos económicos positivos. Porque otorga certeza jurídica asociada al

tratamiento de datos personales, clave para desarrollar el sector, y facilitaría el libre flujo transfronterizo de datos a nivel global, esencial para aprovechar todo el potencial del mercado. Sin embargo, al limitar el uso que se le puede dar a los datos, es poco probable que surjan iniciativas innovadoras en el sector desde Chile. Por ende, la industria de servicios globales y la exportación de servicios (principalmente TICs), podrían ser las principales áreas que se potenciarán con la nueva regulación (porque ya existen).

Lista de referencias

A

Aaronson, S. (2018). What Are We Talking about When We Talk about Digital Protectionism? *World Trade Review*, 18(4), 541-577. doi:10.1017/S1474745618000198.

Aaronson, S. & Leblond, P. (Junio 2018). Another Digital Divide: The Rise of Data Realms and its Implications for the WTO. *Journal of International Economic Law*, 21(2), 245–272, https://doi.org/10.1093/jiel/jgy019.

Accenture y Oxford Economics. (2016). El avance de la economía digital en Chile. Optimizando las capacidades digitales para multiplicar el crecimiento.

Acquisti, A. (2010). The Economics of Personal Data and the Economics of Privacy. Working Paper, CMU.

Acquisti, A. & Brandimarte, L. (2012). The economics of privacy. *The Oxford handbook of the digital economy*, 20.

Acquisti, A. & Varian, H. R. (2005). Conditioning Prices on Purchase History. Marketing Science 24(3), pp. 1–15.

Allen, D., Berg, A., Berg, C., Markey-Towler, B. & Potts, J. (2018). Some Economic Consequences of the GDPR. Economics Bulletin, vol.39, nº2, pp. 785-797.

Asia-Pacific Economic Cooperation [APEC]. (2015). APEC Privacy Framework. Singapur.

Asamblea General de la Organización de las Naciones Unidas. (1948). Declaración Universal de Derechos Humanos.

Asia-Pacific Economic Cooperation [APEC]. (2015). APEC Privacy framework. APEC Secretariat. Singapur.

Athey, S. (2014). *Information, Privacy and the Internet*: An Economic Perspective. CPB Netherlands Bureau for Economic Policy Analysis.

B

Blades, N. & Herrera, F. (2016). An Economic Analysis of Personal Data Protection Obligations in the European Union. 27th European Regional Conference of the International Telecommunications Society (ITS). International Telecommunications Society (ITS). Cambridge, Reino Unido.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences Privacy and the Control Paradox. Social Psychological and Personality Science, 4(3), 340—347.

Broom, D. (24 de junio de 2019). China by numbers: 10 facts to help you understand the superpower today. World Economic Forum. Visto en https://www.weforum.org/agenda/2019/06/china-by-numbers-10-facts-to-help-you-understand-the-superpower-today/ el 1 de marzo de 2020.

Budzyn, A. (2019). Data is the oil of the digital world. What if tech giants had to buy it from us? Visitado el 04-05-2019 en World Economic Forum https://www.weforum.org/agenda/2019/04/data-oil-digital-world-asset-tech-giants-buy-it/.

C

Comisión Nacional de Productividad. (2018). El futuro de las Tecnologías disruptivas en Chile. Santiago, Chile. Capítulo I: Economía y Plataformas Digitales.

Cory, N. (1 de mayo 2017). Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? Information Technology & Innovation Foundation. Visto en https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost el 20 de julio de 2019.

Clement, J. (24 de abril de 2020). Worldwide digital population as of April 2020. STATISTA. Visto en https://www.statista.com/statistics/617136/digital-population-worldwide/ el 1 de marzo de 2020.

Council of Europe. (18 de mayo 1981). Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data. ETS No.180. and 2001 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authoritues and transborder data flows. ETS No. 181.

Comisión Constitución, Legislación, Justicia y Reglamento del Senado. (14 de marzo 2018). Comparado Primer trámite constitucional (Primer informe de comisión) Comisión de Constitución, Legislación, Justicia y Reglamento. Visto en https://senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07 el 27 de abril de 2020.

Constitución Política de Chile. (2005).

D

Dirección General de Relaciones Económicas Internacionales [DIRECON]. (2018). *Anuario de las Exportaciones Chilenas 2018.* Impacto de los tratados de libre comercio. Hacia una política comercial inclusiva. Santiago.

DLA Piper. (31 de diciembre de 2019). Data Protection Laws of the World. China. Visto en https://www.dlapiperdataprotection.com/?t=law&c=CN el 20 abril de 2020.

E

European Commission. (2017). Reflection Paper in Harnessing Globalisation. Bruselas. Publications Office European Union. DOI: 10.2775/41851.

European Commission. (2017). Building a European Data Economy. Bruselas. Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions.

European Data Protection Board [EDPB]. (27 agosto 2018). Statement of the EDPB on the data protection impacts of economic concentration. Visto en https://edpb.europa.eu/our-work-tools/our-documents/autre/statement-edpb-data-protection-impacts-economic-concentration_en el 20 abril de 2020.

European Data Protection Board [EDPB]. (16 de noviembre de 2018). Guidelines 3/2018 on the territorial scope of the GDPR. (Article 3) Version for public consultation. Visto en https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf el 2 de marzo de 2020.

European Data Protection Board [EDPB]. (2019). First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities. Visto en https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf el 2 de marzo de 2020.

F

Fajardo, D. (2019). ¿Qué es un data center y por qué Chile atrae a las gigantes tecnológicas? Pulso. Visto en https://www.latercera.com/pulso/noticia/data-center-chile-atrae-las-gigantes-tecnologicas/539494/ el 3 de marzo de 2020.

Ferracane, M.F. & van der Marel, E. (2018a). Do Data Policy Restrictions Inhibit Trade in Services? Bruselas. European Centre for International Political Economy [ECIPE]. Working Paper 02.

Ferracane, M.F. & van der Marel, E. (2018b). Patterns of Trade Restrictiveness in Online Platforms a first look. Bruselas. European Centre for International Political Economy [ECIPE]. Working Paper 03.

Francis, L. & Francis, J. (2017). Privacy: what everyone needs to know. Oxford University Press.

G

Godel, M., Landzaat, W. & Suter, J. (Mayo 2017). Research and analysis to quantify the benefits arising from personal data rights under the GDPR. Report to the department for culture, media & sport. London Economics. Inglaterra.

Greenleaf, G. (2018). Convention 108+ and the Data Protection Framework of the EU. University of New South Wales Law Research Series.

Global Legal Group Ltda. (2018). The International Comparative Legal Guide to: Data Protection 2018. A practical cross-border insight into data protection law. 2018. 5ta Edición. Inglaterra.

H

I

InvestChile. (2018). Data Centers en Chile: Las ventajas de un país hiper conectado. InvestChile. Visto en http://blog.investchile.gob.cl/bloges/data-centers-en-chile-las-ventajas-de-un-pa%C3%ADs-hiper-conectado el 1 de marzo de 2020.

J

Jia, J., Zhe Jin, G. & Wagman, L. (2018). The short run effects of GDPR on technology venture investment. Working Paper 25248. JEL No. D43,D8,L13,L15,L5. National Bureau of Economic Research. Working paper series.

Jijena, R. (2010, p. 413-431). Actualidad de la protección de datos personales en América Latina. El caso de Chile. *"Revolución informática con Independencia del individuo"*. Disponible en Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM, visto en http://biblio.juridicas.unam.mx/libros/6/2940/27.pdf.

K

L

Lehuedé, H. (2019). Corporate governance and data protection in Latin America and the Caribbean. Production Development series, No. 223 (LC/TS.2019/38), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC), 2019. Visto en https://repositorio.cepal.org/bitstream/handle/11362/44629/S1900395_en.pdf?sequence=1&isAllowed=y el 5 de marzo de 2020.

Lever, G., Yukich, Y. & Cruz, M. (2016). La economía digital en Chile 2016. Centro de Estudios de la Economía Digital, Cámara de Comercio de Santiago.

Ley N° 19.628. Diario Oficial de la República de Chile, Santiago, Chile, 28 de agosto de 1999.

Ley N° 21.096. Diario Oficial de la República de Chile, Santiago, Chile, 16 de junio de 2018.

Ley N° 20.285. Diario Oficial de la República de Chile, Santiago, Chile, 2018.

López, J., Joujean, M. (2017). Digital Trade: Developing a Framework for Analysis. 205 OECD Trade Policy Papers. Visto en http://dx.doi.org/10.1787/524c8c83-en el 17 de febrero de 2020.

M

Meeker, M. (11 de junio de 2019). Internet Trends 2019. Bond Partners. Visto en https://www.bondcap.com/report/itr19/#view/1 el 4 de abril de 2020.

Ministerio de Hacienda. (2017). Informe de Productividad: Proyecto de ley que regula la protección y el tratamiento de los datos personales. Visto en https://open.economia.cl/wp-content/uploads/2019/04/2017.03.15-Datos-Personales.pdf el 2 de marzo de 2020.

Motiwalla, L., Li, X. & Liu, X. (2014). Privacy paradox: Does stated privacy concerns translate into the valuation of personal information? *Pacific Asia Conference on Information Systems (PACIS) (proceedings 281).*

N

Noyes, K. (2016). Four US Companies Rule the world Cloud Infrastructure. Computer World. Visto en https://goo.gl/PirYHB el 2 de febrero de 2020.

O

Organisation for Economic Co-operation and Development [OECD]. (2013). The OECD Privacy Framework. OECD Publishing.

Organisation for Economic Co-operation and Development [OECD]. (11 de julio de 2013). Guía revisada de los Lineamientos de Privacidad de la OCDE.

Organisation for Economic Co-operation and Development [OECD]. (2017). Measuring digital trade: towards a conceptual framework. Francia. Visto en http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=STD/CSSP/WPTGS(2017)3&docLanguage=En el 30 de enero de 2020.

P

Parlamento Europeo & Consejo de la Unión Europea. (1995). Directiva 95/46/CE del Parlamento Europeo y del Consejo. Diario oficial, N° L 281, p. 0031 - 0050. Visto en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN el 1-09-2019.

Parlamento Europeo & Consejo de la Unión Europea. (04 de mayo de 2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Recuperado el 04-04-2020 de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1559205159718&uri=CELEX:32016R0679

Piñera, S. (14 de octubre de 2019). Formula indicaciones al proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la agencia de protección de datos personales. (boletín N° 11144-07). Comisión Constitución, Legislación, Justicia y Reglamento del Senado. Visto en https://senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07 el 25 abril de 2020.

Privacy International. (2017). What its privacy? Visto en https://privacyinternational.org/explainer/56/what-privacy el 4 de marzo de 2020.

Proyecto de ley que "Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales" (Proyecto de Ley N° 11.144-07, 2017).

Purtova, N. (2017). Do property rights in personal data make sense after the big data turn: individual control and transparency. Journal of Law and Economic Regulation, 10(2), 64-78.

Purtova, N. (2018). The law of everything: Broad concept of personal data and future of EU data protection law. Law, innovation and technology. 10:1, 40-81. DOI: 10.1080/17579961.2018.1452176.

Q

R

Reglamento General de Protección de Datos (RGPD). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE (Reglamento general de protección de datos) (texto pertinente a efectos del EEE). Diario Oficial de la Unión Europea, serie L, núm. 119 (4 de mayo de 2016). Recuperado el 04-04-2020 de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1559205159718&uri=CELEX:32016R0679.

Reinsel, D., Gantz, J., & Rydning, J. (Noviembre 2018). The digitization of the world: From edge to core. Recuperado el 04-04-2020 de https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

Roberts, R. (Octubre, 2018). Reporte: Consulta experta sobre la Ley de Protección de la vida Privada de las Personas. Biblioteca del Congreso Nacional de Chile. [BCN]. Visto en https://www.bcn.cl/obtienearchivo?id=repositorio/10221/26703/2/BCN_Consulta_experta_sobre_la_Ley_de_Proteccion_de_la_vida_Privada.pdf el 4 de abril de 2020.

S

Salas, A. (2018). Regulaciones de privacidad de datos online en Chile y Australia: Revisión crítica y desafíos futuros. Latin American Legal Studies. Volumen 3. Página 97-134. 10.15691/0719-9112Vol3a5.

Sampath, P. G. (Marzo 2019). Regulating the digital economy: Dilemmas, trade offs and potential options. Research papers 93. South Centre. Genova, Suiza.

Statista. (2019). Market Capitalization of the Biggest Internet Companies Worldwide as of June 2019 (in billion US dollars). Visto en https://goo.gl/vSba2p el 30 de enero de 2020.

T

Tapscott, D. (1994). *The digital economy: Promise and peril in the age of networked intelligence*. New York: McGraw-Hill.

Turck, M. (2016). The Power of Data Network Effects. Recuperado el 02-04-2020 en http://mattturck.com/2016/01/04/the-power-of-data-network-effects/.

The Economist. (2017a). Fuel of the future: Data is giving rise to a new economy. Londres. The Economist Group Limited. Recuperado el 20-04-2019 en https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy.

The Economist. (2017b). Regulating the internet giants: The world´s most valuable resource is no longer oil, but data. Londres. The Economist Group Limited. Recuperado el 20-04-2019 en https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

The Economist. (2019). Congress is trying to create a federal privacy law. Visto en https://www.economist.com/united-states/2019/02/28/congress-is-trying-to-create-a-federal-privacy-law el 8 de marzo de 2020.

U

United Nations Conference on Trade and Development [UNCTAD]. (2016). Data Protection Regulations and International Data Flows: Implications for trade and development. United Nations Publications. Switzerland.

V

Viollier, P. (2017). El estado de la protección de datos personales en Chile. Derechos Digitales América Latina. Chile.

W

Wallace, N. & Castro, D. (2018). The impact of the EU´S new data protection regulation on AI. Center for data innovation. Recuperado el 17-05-2019 en http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf.

World Economic Forum [WEF]. (2018). Data Policy in the Fourth Industrial Revolution: Insights on personal data.

X

Y

Z