INFORME DE PRODUCTIVIDAD

Proyecto de Ley que Regula la Protección y el Tratamiento de los Datos de Personales

Mensaje N°: 001-365

Ministerio de Hacienda

15.03.2017

Índice de Contenidos

I. Descripción del problema

- Ámbito de aplicación de la regulación
- Implicancias de no realizar las modificaciones regulatorias

II. Objetivos del proyecto

- Descripción de la propuesta regulatoria
- Evaluación de los objetivos
- Experiencia comparada

III. Alternativas de política consideradas

IV. Beneficios del Proyecto de Ley

1. Beneficios de la Protección de la Privacidad
2. Fomento al desarrollo de la industria de servicios globales (*Offshoring*)
3. Promoción de la industria de servicios en línea
4. Fomento a la competencia en los mercados
5. Simplificación de trámites en el Estado
6. Reducción en los costos de reclamación para los titulares de datos personales

V. Posibles costos del Proyecto de Ley

1. Implementación de la Agencia de Protección de Datos Personales
2. Costos del manejo de los datos personales
3. Costos de acceso a información de actuales y potenciales clientes

VI. Conclusiones

I. Descripción del problema

La reducción en los costos de almacenamiento de la información gracias a los rápidos avances tecnológicos de las últimas décadas, ha hecho posible la obtención, el almacenamiento y el análisis de una gran cantidad de datos personales a costos cada vez más bajos. Hoy en día las empresas pueden mantener un registro detallado de todas las transacciones de sus clientes y los sitios web tienen la capacidad de almacenar información de las masivas visitas que reciben por día. Existen empresas además que recopilan datos únicos de distintas fuentes para combinarlos y elaborar perfiles detallados de los individuos, que son posteriormente vendidos a terceros para el desarrollo de nuevos negocios.

Esta realidad ha generado la necesidad de establecer las condiciones regulatorias que permitan a las personas proteger sus datos personales frente a una intromisión no consentida de terceros, sean éstos públicos o privados. En el centro de las demandas de los titulares de datos personales está el respeto a ciertos derechos, como son el derecho de acceso a su información, el derecho a rectificar datos que son inexactos, el derecho a eliminar su información en determinadas circunstancias y de oponerse al tratamiento automatizado de su información para ciertos fines. Los responsables del tratamiento de datos personales, por su parte, requieren un cuerpo legislativo coherente que establezca las condiciones bajo las cuales los datos personales pueden ser tratados de forma lícita.

Hoy la regulación sobre protección y uso de datos de carácter personal de las personas naturales está contenida en la Ley N° 19.628, del año 1999, sobre protección de la vida privada. Si bien esta ley constituyó un gran avance al momento de su publicación, siendo Chile el primer país latinoamericano en adoptar un marco regulatorio en la materia, existe amplio consenso entre los actores políticos e institucionales, organismos internacionales, académicos, entidades de la sociedad civil, empresas y la sociedad en general, que la actual normativa ha comenzado a ser insuficiente. La obsolescencia de algunos de sus criterios u orientaciones regulatorias, junto con la ausencia de una autoridad de control y de un diseño institucional adecuado la han llevado a perder eficacia en su función de protección de la privacidad de las personas en su interacción con otros y con el propio Estado.

Además, cuando Chile firmó el Convenio de Adhesión a Organización para la Cooperación y el Desarrollo Económico (OCDE) en 2010, se comprometió a seguir avanzando en las reformas de aquellas materias que son ejes para el desarrollo social y económico, tales como la protección de la privacidad y el flujo transfronterizo de datos. Dicho compromiso se cumple con el envío al Congreso de este Proyecto de Ley.

De esta forma, se propone avanzar en una nueva legislación que perfeccione y complete los vacíos de la actual normativa, equilibrando de forma adecuada la protección de los derechos y libertades de las personas que son titulares de los datos personales con el aseguramiento de la libre circulación de la información.

Ámbito de aplicación de la regulación

La regulación que se propone tendrá impacto en todas las personas naturales o jurídicas, responsables de datos, que realicen tratamiento de datos personales en Chile.

Los grupos que se ven impactados son los siguientes:

- **Sector público:** todos los órganos públicos que forman parte de la Administración del Estado, el Congreso Nacional, el Poder Judicial, los tribunales especiales creados por ley y los órganos públicos dotados de autonomía constitucional.

- **Sector privado**: todos las empresas (incluyendo micro, pequeñas, medianas y grandes empresas) y las personas naturales que en el desarrollo de una actividad económica realicen el tratamiento de datos personales.

  De acuerdo a información que se obtiene de la base de afiliados al Seguro de Cesantía, que maneja la Administradora de Fondos de Cesantía (AFC), existen alrededor de 332 mil empresas en el país (promedio 2016). De este total, alrededor de 260 mil son microempresas, 44 mil pequeñas empresas, 9 mil empresas medianas y sólo 3 mil son empresas de gran tamaño. Todas ellas, en mayor o menor medida, podrían verse afectadas por esta regulación.

- **Sociedad civil**: las ONGs, las organizaciones comunitarias, corporaciones, fundaciones y asociaciones, los partidos políticos, las asociaciones gremiales, los sindicatos, las asociaciones de consumidores, los centros de estudios, las universidades, organismos de educación y cualquier otra entidad que no desarrolle una actividad económica y que trate datos personales.

La regulación afectará también a todas las personas cuyos datos personales sean tratados en Chile, garantizándoles una serie de derechos en relación al manejo de sus datos. En la práctica, todas las personas que utilizan medios electrónicos para realizar transacciones, transitan por autopistas urbanas, emplean tarjetas de identificación o registro magnético, navegan en Internet, se registran mediante nombres de usuario y una clave en diferentes sitios web, entregan su RUT en distintos comercios para la acumulación de puntos o son parte del Registro Social de Hogares que aplica el Ministerio de Desarrollo Social, entre otras actividades, serán afectadas por la nueva regulación.

En cuanto a las actividades sujetas a la regulación, el proyecto involucra todo tratamiento de datos personales que realicen las personas naturales o jurídicas, incluidos los órganos públicos, las empresas y entidades de la sociedad civil o del tercer sector que no se encuentre regido por una ley especial. Respecto de los tratamientos de datos personales sujetos a una ley especial, se establece el carácter supletorio de esta normativa; es decir, se aplica en todos aquellos casos que no exista una regla especial.

Se encuentran excluidos de este régimen regulatorio el tratamiento de datos personales que se realice en el ejercicio de las libertades de emitir opinión y de informar regulado por las leyes especiales (ley de la Prensa) y el tratamiento de datos que efectúen las personas naturales en relación con sus actividades personales.

Implicancias de no realizar las modificaciones regulatorias

La opción política pública de 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.

El hecho de que el país no cuente con adecuados estándares internacionales de protección de datos frena el desarrollo de las exportaciones de servicios y, en particular, el desarrollo de la industria de servicios globales. A su vez, esto impacta en la atracción de inversiones, el desarrollo y la innovación tecnológica, y en la generación de capital humano avanzado. Asimismo, los consumidores, que pueden expresar reticencias cuando tengan la opción de utilizar servicios en línea cuando no reciben las garantías suficientes de un manejo seguro de sus datos personales, se desalienta el desarrollo de un sector emergente con gran potencial de crecimiento.

En los últimos años se han desarrollado diversas acciones para intentar subsanar, en parte, las falencias del marco normativo provisto por la Ley 19.628 de 1999 y aminorar los costos que esta situación implica. Entre estas acciones se considera un conjunto de modificaciones legales a la Ley 19.628; la utilización de modelos de autorregulación y buenas prácticas en el tratamiento y protección de los datos personales; y la judicialización de los casos de manejo ilícito de los datos personales. No obstante, ninguna de estas alternativas, en forma aislada o en su conjunto, ha sido suficiente para responder a los crecientes desafíos que esta materia involucra.

Desde su publicación, la Ley 19.628 se ha modificado en cinco ocasiones, en diversos ámbitos, con el fin de perfeccionar criterios u orientaciones regulatorias inadecuadas y

completar algunos vacíos de la legislación[1]. Asimismo, están en tramitación más de 60 iniciativas legislativas, originadas mayormente en mociones parlamentarias, que han intentado regular aspectos como el tratamiento de datos personales, el tratamiento del spam, y el control del marketing directo, entre otras muchas materias. El principal problema es que estas modificaciones no han sido parte de un esfuerzo ordenado y sistemático por generar una legislación moderna que se adecue a los estándares internacionales, como se intenta hacer en este proyecto de ley.

Por otra parte, los modelos de autorregulación asumidos por los propios responsables de datos, sin mecanismos de verificación, control y seguimiento, han sido escasos y con bajo impacto. Si bien estos mecanismos les dan mayor flexibilidad a los responsables de datos en el cumplimiento de la normativa, tienen por lo mismo una eficacia bastante limitada. Por último, la judicialización de los casos implica altos costos para los intervinientes y para el Estado y genera importantes grados de incertidumbre para los responsables de datos personales respecto a cuándo es lícito el tratamiento que realizan.

II. Objetivos del proyecto de ley

Este proyecto de ley busca avanzar en una nueva legislación que perfeccione y complete los vacíos de la actual normativa, equilibrando de forma adecuada la protección de los derechos y libertades de las personas que son titulares de los datos personales con el aseguramiento de la libre circulación de la información. Además, busca incorporar un sistema institucional y de incentivos que asegure la aplicación y cumplimiento de la ley, siempre recogiendo los estándares internacionales contenidos en la legislación comparada. En concreto, persigue los siguientes objetivos:

1. Establecer condiciones regulatorias que permitan reforzar los derechos de los titulares de los datos personales.

2. Dotar al país de una normativa coherente con los estándares y compromisos internacionales, especialmente aquellos adquiridos con el ingreso de Chile a la OCDE.

3. Incrementar los estándares legales de Chile en el tratamiento de datos personales para transformarlo en un país con niveles adecuados de protección y seguridad.

[1] Entre estas modificaciones se incluyen: Ley 19.812, de 2002, que introduce una serie de modificaciones para lograr una mayor reinserción laboral de aquellas personas con registros de morosidades y documentos protestados; Ley 20.285, de 2008, sobre Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado; Ley 20.463, de 2010, que suspende por un determinado plazo la información comercial de las personas cesantes. Ley 20.521, de 2011, que introduce modificaciones para garantizar que la información entregada a través de predictores de riesgo sea exacta, actualizada y veraz; Ley 20.575, de 2012, que establece el principio de finalidad en el tratamiento de datos personales.

4. Definir estándares regulatorios y condiciones para legitimar el tratamiento de datos personales por parte de los órganos públicos, compatibilizando el cumplimiento de la función pública y los derechos de los ciudadanos.

5. Contar con una autoridad de control de carácter técnico y una institucionalidad pública que asuma los desafíos regulatorios y de fiscalización en materia de tratamiento de datos personales.

Descripción de la propuesta regulatoria

Para lograr los objetivos antes descritos el Proyecto de ley propone los siguientes cambios a la normativa vigente:

1. Se incorporan un conjunto de principios rectores en materia de protección y tratamiento de datos personales reconocidos en la legislación comparada.

2. Se refuerzan y amplían los derechos de los titulares de datos personales. Se le reconocen los derechos ARCO[2], derecho a la portabilidad de los datos y "derecho al olvido" en relación a los datos sobre infracciones penales, civiles, administrativas y disciplinarias.

3. Se establece un procedimiento directo y eficaz para que una persona pueda recurrir directamente ante el responsable de datos.

4. Se establece el consentimiento del titular como la principal fuente de legitimidad del tratamiento de los datos personales.

5. Se regula las obligaciones, deberes y del régimen de responsabilidades al que se sujetan las personas naturales o jurídicas que realizan tratamiento de datos personales (responsables de datos).

6. Se adoptan nuevos estándares normativos para el tratamiento de los datos personales sensibles y establecimiento de una regulación específica para cierto tipo de datos sensibles y para algunas categorías especiales de datos personales.

---

[2] Sigla que identifica los siguientes derechos: Acceso a la información personal que está siendo tratada, Rectificación de datos inexactos o incompletos, Cancelación de datos en casos particulares y Oposición al tratamiento de su información para ciertos fines.

7. Se establece una protección y regulación especial para el tratamiento de los datos personales de niños, niñas y adolescentes.

8. Se introduce una regulación particular para el flujo transfronterizo de datos personales, que se ajusta plenamente a los estándares y recomendaciones de la OCDE.

9. Se modernizan los estándares regulatorios para el tratamiento de datos personales por parte de organismos públicos. El tratamiento de datos personales y la cesión de los mismos será lícito sólo cuando se realice para el cumplimiento de sus funciones legales; por ejemplo, para otorgar beneficios sociales o evitar la duplicidad de trámites. Se define además un procedimiento de reclamación administrativa y de tutela judicial efectiva para el ejercicio y protección de estos derechos, y se establece que es la autoridad o jefe superior del órgano el responsable de un adecuado tratamiento de los datos personales de acuerdo a la ley.

10. Se crea una institución especializada y de carácter técnico, llamada Agencia de Protección de Datos Personales encargada de velar por el cumplimiento de la normativa relativa al tratamiento de datos personales y su protección, con facultades para regular, supervisar, fiscalizar y sancionar los incumplimientos. Se consagra un modelo de coordinación regulatoria cuando ésta deba dictar una instrucción o norma con efectos en los ámbitos de competencia del Consejo para la Transparencia.

11. Se contempla un catálogo específico de infracciones a los principios y obligaciones establecidos en la ley cometidas por los responsables de datos, que se califican atendida su gravedad. De forma coherente, se establecen sanciones que van desde la amonestación escrita a multas que oscilan entre 1 y 5.000 UTM. En casos excepcionales se contempla el cierre o clausura de las operaciones de tratamiento de datos.

Evaluación de los objetivos

El cumplimiento de los objetivos de este proyecto de ley se podrá realizar a través de distintos medios. Primero, la Agencia de Protección de Datos Personales, en virtud del ejercicio de su facultades (letras c) y d) del artículo 31), podrá requerir información a los responsables del tratamiento de datos personales y efectuar un seguimiento de la forma en que éstos ajustan sus procedimientos, a fin de dar un debido cumplimiento a la ley. Esta información permitirá realizar un análisis cualitativo de los efectos de la regulación para un manejo lícito, controlados e informado de datos personales.

Segundo, como resultado de las facultades de fiscalización y sancionatorias de la Agencia, se podrán obtener estadísticas detalladas del número y monto de las multas cursadas, el tipo de conducta constitutivo de infracción, el tamaño del perjuicio producido en términos del número de titulares afectados y los beneficios obtenidos, además del número de reclamos que formulen los titulares de datos. En conjunto con las características de los responsables de datos personales infractores (por ejemplo, tamaño, sector económico, volumen y finalidad de los datos tratados), se podrá realizar un seguimiento y un análisis cuantitativo del nivel de cumplimiento de la regulación y su efectividad distinguiendo por tipo de empresa responsable del tratamiento de datos personales. Esta información permitirá evaluar también el efecto de las sanciones como medio de disuasión.

Tercero, el proyecto de ley incorpora un modelo de prevención de infracciones, con mecanismos de verificación, control y seguimiento, al que se podrán acoger todos los responsables del tratamiento de datos personales. Dado que será la Agencia la encargada de revisar que el modelo tenga los estándares adecuados, podrá recopilar y sistematizar información relevante para la evaluación del cumplimiento de los objetivos del proyecto.

Por último, se espera que esta regulación tenga efectos económicos en el país en la medida que mejore la calidad de la normativa que resguarda el respeto a la privacidad y la protección de datos personales. Esto podría traducirse en un aumento de las exportaciones de servicios, en particular, de la industria de servicios globales, y de la inversión en estos sectores. Asimismo, se podría observar un aumento del empleo en los sectores relevantes o que se produzca un aumento de los servicios en línea, entre otras cosas. En función de estas variables será posible realizar una evaluación de los efectos de la regulación, no sólo desde una perspectiva temporal sino también en relación a otros países.

Experiencia comparada

A nivel internacional existen dos corrientes principales en torno a la protección de los datos personales. Uno es el modelo europeo que establece como un derecho fundamental "el derecho a la protección de los datos personales"; por lo tanto, se reconoce como derecho autónomo, independiente del derecho a la privacidad. Por su parte, el modelo estadounidense enfatiza la protección de la vida privada, otorgando amplia autonomía a las personas para controlar su información, sin entorpecer la libre circulación de la misma.

Por su parte, los países miembros de la OCDE elaboraron y adoptaron las *Directrices sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales* del organismo. Aunque no son jurídicamente vinculantes, han sido reconocidas como una declaración de los contenidos y principios esenciales que deben guiar la privacidad de los datos

personales y recoger los miembros de la OCDE en sus normativas internas. Además, al establecer una estrategia común, permite evitar inconsistencias en las legislaciones internas de protección de datos personales, que podrían afectar la libre circulación de los datos y limitar los beneficios económicos del flujo transfronterizo de información.

El proyecto de ley de Protección de Datos Personales actualiza y moderniza el marco normativo e institucional incorporando a la legislación nacional un conjunto de principios rectores que han sido reconocidos en las *Directrices* de la OCDE y en los modelos regulatorios europeo y estadounidense.

Esto se traduce en que la propuesta regulatoria de esta iniciativa se establece que el tratamiento de los datos personales de las personas naturales se realice con el consentimiento del titular de estos datos o en los casos que autorice la ley, reforzando la idea que los datos personales deben estar bajo la esfera de control de su titular, como se establece en el modelo normativo estadounidense. Esto favorece su protección frente a toda intromisión de terceros y establece las condiciones regulatorias bajo las cuales los terceros, personas naturales o jurídicas, empresas u organizaciones públicas y privadas, pueden efectuar legítimamente el tratamiento de tales datos, asegurando estándares de calidad, información, transparencia y seguridad.

Además, se incorporan a la legislación interna un conjunto de principios rectores que han sido reconocidos en las *Directrices* de la OCDE y en el derecho europeo, que inspiran la regulación de las operaciones de tratamiento de datos personales: principio de licitud del tratamiento, principio de finalidad; principio de proporcionalidad; principio de calidad; principio de responsabilidad; principio de seguridad; principio de información. Además, en línea con la normativa europea, se establece una autoridad de control encargada de velar y fiscalizar el cumplimiento de la normativa relativa al tratamiento de datos personales y su protección.

De esta forma, esta regulación equilibra la protección de los derechos y libertades de las personas que son titulares de los datos personales, especialmente el respeto y protección a la vida privada e intimidad, con la libre circulación de la información, asegurando que las reglas de autorización y uso que se establezcan no entraben ni entorpezcan el tratamiento lícito de los datos por parte de los personas, organismos y empresas.

En la actualidad, todos los países miembros de la OCDE tienen una legislación sobre protección de datos personales que se alinea con las directrices de la organización, con excepción de Chile y Turquía. Así, este proyecto de ley permite cumplir un compromiso con la OCDE, adoptando las mejores prácticas internacionales y situándose a la altura de las legislaciones más avanzadas en materia de protección de la privacidad y del flujo transfronterizo de datos personales.

III. Alternativas de política consideradas

Esta propuesta regulatoria es una ley marco que actúa como regla general de aplicación, esto es, aquellos tratamientos de datos que no estén sometidos a una regla especial, se rigen por esta ley y en todo aquellos casos que estos ordenamientos particulares no regulen, se rigen supletoriamente por esta ley. Lo anterior implica que no existe duplicidad normativa o conflicto de ley, ya que esta normativa es de carácter general, pero prevalecen por sobre ella las normas especiales[3]. Respecto de la regulación aplicable al sector público, el proyecto de ley consagra dos normas de coordinación regulatoria con el objeto de evitar duplicidades, contradicciones o vacíos normativos.

En cuanto a las alternativas regulatorias para la protección de datos personales se tuvo a la vista las dos corrientes principales en la materia (modelo europeo y estadounidense, ya descritos). Reconociendo las virtudes de ambos modelos, y tomando en consideración que la Constitución Política de la República establece como un derecho fundamental de las personas el respeto y protección a su vida privada, se optó por un marco normativo que refuerza la protección de los derechos y libertades de las personas que son titulares de los datos personales, especialmente el respeto y protección a la vida privada e intimidad, pero relevando la importancia de no entorpecer la libre circulación de la información, con reglas de autorización y uso adecuadas que permitan un tratamiento lícito de los datos por parte de los personas, organismos y empresas.

Para el cumplimiento de la regulación se optó por la creación y determinación de una autoridad de control, con facultades para regular, supervisar, fiscalizar y sancionar los incumplimientos, siguiendo la orientación del modelo europeo. EE.UU., en cambio, tiene un sistema jurídico de precedentes y con amplia tutela judicial.

En este sentido, existían dos opciones institucionales: asignarle las funciones fiscalizadora, sancionadora y normativa a alguna agencia pública existente (como el Consejo para la Transparencia, CplT) o crear una nueva agencia pública.

Al respecto, la experiencia internacional indica que las facultades de vigilancia o supervigilancia en relación a la protección de datos están radicadas en la gran mayoría de los países en agencias con responsabilidad exclusiva sobre el derecho de protección de datos. Entre estos países se pueden encontrar Australia, Austria, Bélgica, Bulgaria, Canadá, Croacia, Dinamarca, España, Finlandia, Francia, Grecia, Holanda, Irlanda, Italia,

[3] Los órganos públicos que actualmente tienen normativas especiales para el tratamiento de datos personales son la Superintendencia de Pensiones para el seguro de cesantía; Ministerio de Desarrollo Social para información personal para estratificación social;, aquellos encargados de la persecución penal, respecto de la investigación y sanción de delitos; el Servicio de Impuestos Internos para la fiscalización del cumplimiento tributario, entre otros.

Nueva Zelandia, Portugal y Suiza. Si bien hay ejemplos de países que han adoptado la duplicidad de funciones al interior de sus instituciones, como son los casos de México y Reino Unido, las dos son experiencias muy distintas a la que se propone en Chile.

Por otra parte, se debe considerar que los derechos de acceso a la información y de protección de datos son bienes jurídicos que por su naturaleza en muchas oportunidades pueden entrar en conflicto. Para precaver esta eventualidad, al sistema jurídico y político le corresponde generar los mecanismos para que la resolución de este conflicto tenga un cauce institucional, un procedimiento racional y competencias diferenciadas. De ahí la importancia de contar con instituciones diferentes. En un Estado de Derecho estos conflictos son resueltos, en última instancia, por los Tribunales de Justicia, pero teniendo en cuenta la opinión especializada de dos organismos diferentes (uno que pugna en favor de la transparencia en la información pública y otros que actuaría en favor de la protección de la información personal de una persona determinada). En cambio, si existiera una sola institución encargada de velar simultáneamente por la protección de datos y el acceso a la información, uno de estos dos derechos podría quedar desprotegido.

Un aspecto crítico que favorece la posición que deban existir dos instituciones distintas es que los ámbitos regulatorios de la protección de datos y del acceso a la información son muy distintos, lo que se refleja en una serie de factores:

- **Actores**: los actores sujetos a las reglas y obligaciones de acceso a la información y transparencia son principalmente entidades públicas o entidades privadas que cumplen una función pública y reciben aportes del Estado. Los actores que tratan datos personales son personas y entidades públicas o privadas.

- **Principios**: Los principios que orientan a las instituciones que regulan estas actividades tienen orígenes y focos distintos, incluso pueden ser contradictorios. El acceso a la información tiene como principios centrales de actuación la transparencia y el acceso a la información pública. En tanto que la protección de datos se centra en el consentimiento de la persona o titular (tratamiento controlado) y en el uso de la información (principios de licitud y finalidad del tratamiento).

- **Funciones y regulaciones**: El ámbito regulatorio de la protección de datos está orientado hacia la generación de estándares normativos que favorezcan un tratamiento de datos controlado, seguro y con amplios grados de autonomía personal para los titulares de datos. En el acceso a la información el foco de la regulación está en el ejercicio de la función pública con transparencia,

promoviendo el conocimiento de los procedimientos, contenidos y decisiones que se adopten en su ejercicio.

- **Especialización**: Las regulaciones en el ámbito del acceso a la información y la transparencia exigen un alto nivel de conocimiento técnico en los modelos de toma de decisiones, procesos y actividades de los órganos de la Administración del Estado. Las regulaciones relativas a la protección de datos exige altos niveles de conocimiento en los mercados de la información personal, el intercambio de datos y la interacción con las nuevas tecnologías de la información (*big data*, internet de las cosas, dispositivos móviles inteligentes, entre otros).

- **Conflictos de intereses**: La institucionalidad ligada a acceso a la información está pensada principalmente en su independencia frente al Poder Ejecutivo. En el caso de la protección de datos los principales conflictos de intereses se darán con el sector privado, por ende el problema se torna mucho más complejo.

En consideración a los planteamientos antes presentados, el Ejecutivo en este proyecto de ley optó por un modelo de autoridad basado en el control especializado y con altos estándares técnicos, que le otorga a la Agencia de Protección de Datos Personales una única función de protección de datos personales.

IV. Beneficios del proyecto de ley

El principal objetivo de este proyecto de ley es salvaguardar el respeto y la protección de los derechos y las libertades de las personas; en particular, el derecho a la privacidad frente a una intromisión no consentida de terceros, sean estos públicos o privados y, regular el tratamiento ilícito de la información de los titulares de datos.

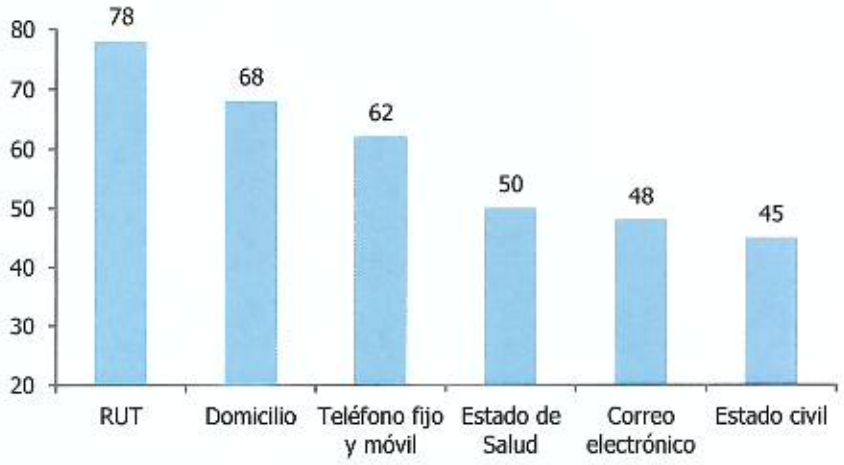
La literatura reconoce un conjunto de *trade-offs* económicos asociados a la difusión y protección de datos personales. Sin embargo, no todos estos *trade-off* tienen una dimensión monetaria explícita. En particular, la protección de la privacidad incide en el bienestar de las personas de manera no sólo intangible, sino que muchas veces no medible. Más allá de esto, se puede distinguir una serie de beneficios económicos que se desprenden de avanzar en una nueva legislación que garantice un adecuado tratamiento de los datos personales.

Los beneficios más relevantes a destacar y que son analizados en este informe son los siguientes:

1. Beneficios de la Protección de la Privacidad

Uno de los principales beneficios del proyecto de ley dice relación con el efecto en bienestar que se deriva de la mayor protección de la privacidad. Estudios de opinión realizados en distintos países muestran que los consumidores tienen una preocupación especial por la privacidad de su información personal[4]. Un estudio del Consejo para la Transparencia (CPLT), muestra que las personas se preocupan del cuidado de su información personal, especialmente cuando se refiere a su RUT, domicilio, y teléfono fijo y móvil (Gráfico 1).

Gráfico 1: Porcentaje de las personas que cuida distintos tipos de información personal, 2014



Fuente: Protección de Datos Personales en el Manejo de Datos de Investigación realizado Organismos Públicos, Unidad de Estudios y Publicaciones, Dirección de Estudios, Consejo para la Transparencia, 2015.

Una valoración económica experimental de los datos personales se realizó para el caso mexicano. Una persona valora en hasta US$ 253 la información altamente sensible –RUT e información bancaria- mientras su valoración cae hasta US$ 6 cuando se trata

[4] En 2000, un estudio de la Comisión Federal del Comercio (FTC, por sus siglas en inglés) reportó que 67% de los consumidores estaban "muy preocupados" por la privacidad de la información personal que entregan en línea. En 2005, en una encuesta de la cadena de noticias CBS en EE.UU., la mayoría de los estadounidenses declaró que su privacidad estaba "en peligro". Asimismo, en 2009, una encuesta de Turow et al. (2009) mostró que la mayoría de los estadounidenses se resisten a recibir publicidad "a la medida".

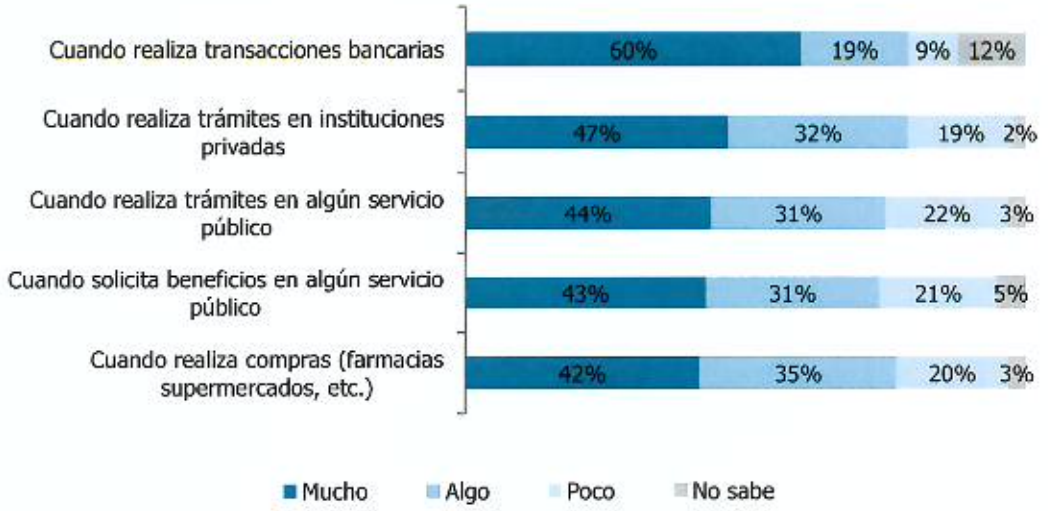
simplemente de su información básica. Utilizando información contenida en pólizas de seguros para proteger a las personas contra el robo de su identidad, u otras herramientas se puede obtener otra aproximación de la valorización que dan las personas a su información personal. Así, por ejemplo, en México, las pólizas para proteger el robo de la identidad se transan en US$ 168, a su vez, las herramientas para eliminar registros cuestan US$ 152 y un *software* de navegación para proteger la identidad vale US$ 108[5].

Una encuesta realizada en México, con una metodología precisa para medir la disposición a pagar por la protección de los datos personales y lo que se estaría dispuesto a aceptar (recibir) por la venta de los propios datos personales, muestra que estos están en torno a US$ 656 y US$ 1.525, respectivamente. Es interesante notar que las personas estarían dispuestas a aceptar por la venta de sus datos personales 2,3 veces más que lo que estarían dispuestos a pagar por la protección de los mismos.

El costo del mal uso de la información personal –y por ende, el beneficio de protegerla—es complejo de medir en la medida que involucra daños tanto tangibles como intangibles, que incluso pueden llegar a manifestarse tiempo después. Calo (2011) distingue entre daños objetivos y subjetivos a la privacidad[6]. Los primeros se vinculan a la pérdida de control de la información personal y a la posibilidad de usar los datos de una persona en contra de ella (por ejemplo, el uso malicioso del RUT de una persona). El estudio del CPLT ya citado muestra que cuando las personas más se preocupan por el mal uso de su información personal es en las transacciones bancarias y en trámites con instituciones privadas (empresas de servicios, grandes tiendas, etc.) (Gráfico 2). Los daños subjetivos se derivan de la percepción de observación indeseada, que pueden generar ansiedad, incertidumbre e incluso temor.

[5] AMIPCI (2014). Estudio sobre el Valor Económico de los Datos Personales.
[6] Calo, R. (2011). The boundaries of privacy harm. *Indiana Law Journal 86.*

Gráfico 2: Situaciones en las cuales las personas se preocupan de su información personal, 2014



Fuente: Protección de Datos Personales en el Manejo de Datos de Investigación realizado Organismos Públicos, Unidad de Estudios y Publicaciones, Dirección de Estudios, Consejo para la Transparencia, 2015.

La existencia de mercados secundarios de datos de consumidores también puede producirles externalidades negativas. Esto, ya sea porque la empresa responsable de los datos extrae todo el beneficio de la información de los consumidores para fines comerciales o publicitarios, o porque obtiene todas la ganancias de transferir la información a terceros, pero sin internalizar los costos para los consumidores de relevar esta información. Dado que los consumidores no tienen cómo saber quién divulga su información o incluso cómo es cruzada con otras fuentes de datos, no son capaces de penalizar adecuadamente a la empresa que ilícitamente hizo uso de su información (Swire y Litan, 1998[7]). En términos económicos, la empresa internaliza las ganancias de usar la información de sus consumidores, pero externaliza varios de los costos.

Por la naturaleza incierta del costo de la privacidad, las personas tienen muchas dificultades para poder cuantificarlos y evaluarlos adecuadamente. No obstante, esto no significa que no existan; pueden ser eventos con alta probabilidad y bajo impacto para las personas (por ejemplo, el *spam*) o materializarse como eventos con un impacto alto pero con baja ocurrencia probabilística (por ejemplo, rechazo de un crédito hipotecario por suplantación de identidad). En cualquier caso, ya sea por su bajo impacto o escasa

[7] Swire, P. P. y R. E. Litan (1998). *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*. Washington, DC: Brookings Institution Press.

probabilidad de ocurrencia, pueden ser ignorados a nivel individual, aunque en el agregado podrían causar un daño social significativo.

2. Fomento al desarrollo de la industria de servicios globales (*Offshoring*)[8]

En la actualidad a las empresas extranjeras de servicios globales se les dificulta instalarse en Chile, porque el país no cuenta con adecuados niveles de protección de datos y las empresas no tienen garantías suficientes de un manejo lícito de la información privada tratada dentro del país. Para poder operar hoy en Chile, las empresas de servicios globales solicitan una autorización para tratar datos personales al regulador extranjero del país correspondiente, lo que encarece el proceso y disminuye las ventajas comparativas de Chile para competir en los mercados internacionales. Así, muchas empresas de servicios evalúan el país donde se instalan dependiendo de si cumple o no los estándares en materia de protección de datos establecidos por la OCDE.

Pese a todo, Chile ha tenido un buen desempeño en el desarrollo de la industria de servicios globales y existe un gran potencial para continuar impulsándolo. No sólo porque el *offshore* de servicios es una industria en rápido crecimiento, que casi cuadruplicó su tamaño entre los años 2005 y 2010[9], sino también porque Chile tiene importantes ventajas comparativas en términos de costos, habilidades y clima de negocios. Es uno de los países de la región más avanzados en materia de conexión digital, uso de TIC y capital humano, además de que comparte huso horario con EE.UU, factores todos que son clave para el desarrollo del sector de exportaciones de servicios. De hecho, el 2008 (último año con información disponible), la industria de servicios globales en Chile exportó US$ 843 millones, aportando a la generación de 20.034 puestos de trabajo.

La disminución en las barreras a los flujos transfronterizos de datos, como resultado de la adaptación de la normativa vigente a los estándares internacionales, y su consiguiente impacto positivo en la industria de servicios globales, podría contribuir de manera indirecta a aumentar el empleo y el capital humano calificado. Al mismo tiempo, al incentivar la transferencia de tecnología y diversificar la oferta exportable, reduciría la vulnerabilidad de la economía chilena a los vaivenes de la economía mundial.

---

[8] El *Offshoring* es un modelo de negocios en que las empresas trasladan actividades y/o procesos al exterior, ya sea mediante la constitución de una subsidiaria en el exterior (inversión extranjera directa) o mediante la subcontratación de un tercero extranjero (exportación de servicios). Los servicios globales incluyen una amplia variedad de actividades, que pueden subdividirse en: i) procesos de tecnología de la información, ii) procesos de negocios y iii) procesos de conocimiento, así como actividades verticales específicas por industria. Las empresas realizan operaciones de *offshoring* para reducir costos, así como para mejorar la calidad y diversificar costos.

[9] El mercado global de offshoring pasó de US$ 57,1 billones en 2005 a US$ 201,9 billones en 2010.

3. Promoción de la industria de servicios en línea

El reforzamiento de los derechos de los titulares de datos personales, ya sea a través de un mayor control de la información que los consumidores entregan o una disminución de las vulneraciones a las medidas de seguridad, podría impactar positivamente en el desarrollo de la industria de servicios en línea.

Las vulneraciones a las medidas de seguridad, que ocasionan la destrucción, filtración, pérdida o alteración de sus datos personales o un acceso no autorizado a ellos, tienen costos relevantes para las personas. Esto es, desde los costos económicos que implican operaciones fraudulentas por compras en línea, o el hecho que la simple incertidumbre que genera saber que una empresa no está protegiendo adecuadamente la información puede llevar a no usar un servicio o comprar un producto. De la misma manera, diversos estudios muestran que en la medida que los consumidores tienen mayor control sobre la información que relevan en las redes sociales, por ejemplo, porque pueden ejercer sus derechos ARCO, sienten mayor confianza y tranquilidad para continuar entregando información de ellos mismos.

4. Fomento a la competencia en los mercados por la portabilidad

El derecho a la portabilidad de los datos incentiva la competencia y el desarrollo de nuevos productos, en la medida que obliga a las empresas a entregar toda la información que ellos manejan respecto a un titular de datos personales. Por ejemplo, en el mercado de la telefonía móvil si los consumidores no pueden medir con exactitud cuánto utilizan su teléfono móvil podrían permanecer en un plan, que no es adecuado de acuerdo a su consumo, siendo que buscando en otras compañías podrían encontrar una alternativa que les entregue el mismo servicios a un precio más bajo. Con esta información, los consumidores fuerzan a las empresas a competir por ofrecerles un mejor precio, lo que a su vez se traduce en un aumento en la competencia y en el desarrollo de nuevos productos, así como en el surgimiento de empresas intermediarias que podrían facilitar la búsqueda de mejores tarifas para los consumidores. Precisamente en el caso de las compañías de teléfonos celulares, los consumidores en el Reino Unido perdieron US$ 7,35 billones en 2011 por quedarse en la compañía equivocada.

5. Simplificación de trámites en el Estado

El proyecto de ley regula con precisión la facultad de los órganos públicos para comunicar o ceder datos personales específicos o bases de datos entre organismos públicos, cuando ellos se requieran para un tratamiento que tenga por finalidad otorgar beneficios al titular,

evitar duplicidad de trámites para los ciudadanos o reiteración de requerimientos de información o documentos para los mismos titulares.

6. Reducción en los costos de reclamación para los titulares de datos personales

En los procedimientos administrativos (de tutela de derecho y de infracción de ley) que se establecen en este proyecto de ley (artículos 45 y 46), los titulares de datos personales no deberán incurrir en costos que sí tienen lugar en la ley vigente, tales como la contratación de abogados para presentar recursos ante el juzgado de letras en lo civil y el costeo de trámites tales como las notificaciones judiciales. El titular de datos que se vea afectado en sus derechos da inicio al procedimiento a través de la presentación de una reclamación ante la Agencia de Protección de Datos Personales, proceso que puede realizarse completamente en línea. Esta reducción en los costos de transacción también favorecerá a los responsables de datos personales.

V. Posibles costos del Proyecto de Ley

El principal costo directo de la propuesta regulatoria contenida en este proyecto de ley es la implementación y el funcionamiento de la Agencia de Protección de Datos Personales. Pero existe también otra serie de posibles costos derivados de un cambio en los procedimientos para manejar los datos personales por parte de los responsables, y de un acceso algo más difícil a la información de los consumidores por parte de las empresas.

Para minimizar estos posibles costos, en el proyecto de ley se establece una gradualidad en la implementación de la regulación y se establece un modelo de prevención de infracciones, a cargo de la Agencia de Protección de Datos. La adopción de modelos de cumplimiento implica, en el mediano plazo, importantes ahorros en los costos administrativos, reducción de contingencias y la generación de una cultura institucional que previene y anticipa riesgos, además de promover el cumplimiento de la ley.

Los costos más relevantes a destacar y que son analizados en este informe son los siguientes:

1. Implementación de la Agencia de Protección de Datos Personales

La propuesta de creación de la Agencia de Protección de Datos Personales tendrá un mayor gasto fiscal en régimen de $ 1.428.876 miles, a partir del segundo año de vigencia de la ley. Respecto a la distribución de estos gastos, el Cuadro 1 presenta el desglose para año 1 y años siguientes en régimen.

Cuadro 1: Distribución de gastos

(miles de pesos de 2017)

Conceptos/Años	Año 1	Año 2 y en régimen
Remuneraciones	711.401	1.166.196
Gasto corriente	169.057	262.680
Inversión inicial	417.560	-
Total Gastos	**1.298.018**	**1.428.876**

Fuente: Informe Financiero N° 021 – 15/03/2017.

Tal como señala el informe financiero del proyecto de ley, la Agencia de Protección de Datos Personales, contará con una Dirección Nacional, 3 Divisiones (Fiscalización y Promoción, Regulación y Jurídica), además de un Departamento de Administración, con 21 funcionarios ingresando el primer año y 33 a partir del segundo (Cuadro 2). Asimismo, se requerirá una inversión inicial para la adquisición de equipamiento de oficinas e informática, así como habilitación de oficinas.

Cuadro 2: Estructural del personal y costos

(miles de pesos de 2017)

Cargos	Cantidad	Grados	Costo Mensual	Costo Anual
Director Nacional	1	1C	7.773	93.281
Jefes de División	4	3	20.464	245.567
Jefes de Departamento	1	4	4.610	55.324
Jefes de Subdepartamento	2	5	7.198	86.370
Profesionales	20	4°-9°	53.762	645.140
Secretarias	3	12°-20°	2.202	26.421
Chofer	1	18	693	8.321
Auxiliar	1	24	481	5.772
Total	**33**		**97.183**	**1.166.196**

Fuente: Informe Financiero N° 021 – 15/03/2017.

2. Costos del manejo de los datos personales

La regulación propuesta podría generar un aumento en los costos administrativos de los responsables de datos para cumplir con la regulación. Estos costos podrían clasificarse en 3 tipos:

a. **Gestión de los datos:** Los responsables deberán mejorar la gestión de los datos personales implementando mecanismos y herramientas tecnológicas que permitan que el titular ejerza sus derechos en forma expedita, ágil y eficaz; deberán reportar a la Agencia las vulneraciones a las medidas de seguridad; deberán mantener permanentemente a disposición del público una serie de datos respecto a los datos que manejan y su política de tratamiento de datos personales.

b. **Atención de reclamos**: El proyecto establece plazos bien definidos y acotados para que los responsables de datos respondan a los requerimientos de los titulares de datos.

c. **Medidas de prevención y servicios de *compliance***: El proyecto genera incentivos para que los responsables inviertan en detectar el tratamiento de datos riesgosos, mejorar la trazabilidad de los procesos y determinar

mecanismos adecuados para detectar filtraciones de datos. Durante los primeros meses de adaptación a la nueva regulación, los responsables de datos podrían encontrar óptimo contratar empresas de *compliance*[10].

3. Costos de acceso a información de actuales y potenciales clientes

El eventual aumento en los costos de acceder a la información de potenciales clientes podría generar problemas de riesgo moral y selección adversa en algunos mercados donde existen asimetrías de información[11]. Asimismo, podría encarecer el costo de obtener información no sólo para las empresas que actualmente operan (incumbentes), sino también para las potenciales entrantes. Como éstas no conocen el mercado, podrían tener mayores dificultades para acceder a sus potenciales clientes, generándose un eventual aumento de las barreras a la entrada, disminuyendo la competencia en favor de las empresas con grandes bases de datos de clientes en dicho mercado y provocando una mayor concentración de los mercados.

Los consumidores se benefician directamente cuando las empresas pueden acceder a flujos relevantes de información respecto a sus preferencias y comportamiento. Las empresas pueden ofrecer a sus clientes recomendaciones personalizadas, que son más útiles para ellos, en base a su comportamiento observado (compras, búsquedas, visitas, clicks en una página web); dirigir más efectivamente su publicidad reduciendo la cantidad de información irrelevante para los clientes o incluso puede entregarles directamente cupones de descuento; y mejorar sus servicios o rediseñarlos para adecuarlos a las necesidades de sus clientes. En este sentido, la limitación del flujo de información podría traducirse en una pérdida de opciones que podrían ser interesantes para los consumidores.

---

[10] Un análisis cualitativo en Hoofnagle (2007) da cuenta de que las empresas en EE.UU. aumentan sus gastos administrativos y en seguridad luego de la publicación de varias leyes que penalizan las filtraciones de datos.

[11] Se produce riesgo moral cuando un individuo toma más riesgo porque sabe que son otras personas las que soportan las consecuencias de los mayores riesgos asumidos. En cambio, se produce selección adversa, previo a la firma de un contrato, cuando la parte menos informada no es capaz de distinguir la buena o mala calidad de lo ofrecido por la otra parte.

VI. Conclusiones

El acelerado desarrollo tecnológico, la masificación en el uso de las tecnologías de la información, el extendido acceso a internet, la generación y uso de grandes volúmenes de información a través de sistemas automatizados de procesamiento, la expansión del comercio electrónico, sumado a los nuevos desafíos que enfrentan las sociedades en materia de reconocimiento y protección de los derechos de las personas, hacen necesario avanzar en una nueva legislación que perfeccione y complete los vacíos de la actual normativa.

Además, se hace necesario el cumplimiento del compromiso de Chile, adquirido con la OCDE con la firma del Convenio de Adhesión, respecto a seguir avanzando en las reformas de aquellas materias que son ejes para el desarrollo social y económico, tales como la protección de la privacidad y el flujo transfronterizo de datos.

Uno de los principales beneficios del proyecto de ley dice relación con el efecto en bienestar que se deriva de la mayor protección de los derechos y las libertades de las personas, en particular el derecho a la privacidad frente a una intromisión no consentida de terceros, sean estos públicos o privados. Las personas tienen una preocupación especial por la privacidad de su información personal y están dispuestas a desembolsar sumas relevantes de recursos para protegerse frente al mal uso de ésta. Sin embargo, se debe considerar que la protección de la privacidad incide en el bienestar de las personas de manera no sólo intangible, sino que muchas veces no medible, por lo que es complejo estimar su potencial impacto en la economía.

Se puede distinguir una serie de beneficios económicos que se desprenden de avanzar en una nueva legislación que garantice un adecuado tratamiento de los datos personales. Entre ellos, destaca el fomento al desarrollo de la industria de servicios globales, que tiene un tremendo potencial de crecimiento, además de contribuir a generar más empleo y aumentar la demanda por capital humano calificado. Esto también puede contribuir a incentivar la transferencia de tecnología y diversificar la oferta exportable, reduciendo la vulnerabilidad de la economía chilena a los vaivenes de la economía mundial.

Asimismo, el reforzamiento de los derechos de los titulares de datos personales tendrá un impacto en el desarrollo de servicios en línea, y fomentará la competencia en los mercados por la portabilidad de los datos personales. Para éstos también implicará una disminución en los tiempos que dedican a hacer trámites frente al Estado, porque se termina con la duplicidad de trámites o la reiteración de requerimientos de información, en la medida que se establece un procedimiento claro para que los órganos públicos puedan comunicar o cederse información de forma lícita entre ellos. Otra ventaja para los consumidores es que en caso que una persona sienta que sus derechos han sido

vulnerados, puede dar inicio a un procedimiento a través de la presentación de una reclamación ante la Agencia de Protección de Datos Personales, en forma completamente en línea y gratuita. Con la ley vigente, las personas deben incurrir en costos de contratación de abogados para presentar recursos ante el juzgado de letras en lo civil y de trámites tales como las notificaciones judiciales.

En cuanto a los costos de esta regulación, estos se derivan de la implementación y funcionamiento de la Agencia de Protección de Datos Personales y del cambio en los procedimientos para manejar los datos personales por parte de los responsables. Esto podría hacer más difícil el acceso a la información relevante de los consumidores por parte de las empresas; sin embargo, se establece una gradualidad en la implementación de la regulación y un modelo de prevención de infracciones, a cargo de la Agencia de Protección de Datos, para minimizar estos costos.

El modelo regulatorio que se presenta equilibra de forma adecuada la protección de los derechos y libertades de las personas que son titulares de los datos personales, sin entrabar ni entorpecer la libre circulación de la información, para no limitar los beneficios económico del flujo de información.

En suma, los beneficios que trae el cambio regulatorio que contiene este proyecto de ley superan ampliamente los posibles costos asociados a esta propuesta. En este sentido, se justifica plenamente avanzar en esta nueva legislación que perfeccione y complete los vacíos de la actual normativa, y ponga a Chile a la altura de los países más avanzadas en la protección de su información personal.

REPUBLICA DE CHILE
MINISTRO
MINISTERIO DE HACIENDA

RODRIGO VALDÉS PULIDO

Ministro de Hacienda