DOCUMENTO POSICIONAL AMCHAM CHILE

Observaciones al Proyecto de Ley que Regula la Protección y el Tratamiento de los Datos Personales y Crea la Agencia de Protección de Datos Personales

Para ser presentado ante la Comisión de Constitución, Legislación, Justicia y Reglamento de la Cámara de Diputados

Mayo de 2022

Para la Cámara Chileno Norteamericana de Comercio, Amcham Chile, es fundamental que Chile siga avanzando en la construcción de un marco regulatorio robusto y balanceado en materia de protección de datos personales, protegiendo los derechos fundamentales de las personas y permitiendo el desarrollo de emprendimientos y nuevos negocios.

AmCham Chile ha participado en las diversas instancias de discusión de los esfuerzos legislativos para actualizar la Ley 19.628. Consistentemente, hemos comunicado que la industria y el comercio ven la regulación como un desafío positivo y su ausencia como una oportunidad constructiva. Por el contrario, el escenario que es percibido como una desventaja, es aquel con una regulación que carece de claridades, y dificulta ciertos grados de predictibilidad de las decisiones comerciales.

Por ello, apoyamos el desarrollo de una regulación coherente y orgánica, para lo cual es fundamental avanzar con la tramitación del proyecto actualmente en debate en la Comisión de Constitución, Legislación, Justicia y Reglamento de la Cámara de Diputados.

Creemos relevante referirnos a la discusión que se ha dado en relación con la institucionalidad consagrada en el presente proyecto de ley. En este sentido, destacamos el acuerdo y el avance logrado en el año 2021, prevaleciendo la opinión de la academia, expertos en protección de datos y parlamentarios, lo cual llevó al ejecutivo a consagrar una Agencia de Protección de Datos, como una corporación autónoma de derecho público, de carácter técnico, descentralizado, con personalidad jurídica y patrimonio propio, que se relacionará con el Presidente de la República a través del Ministerio de Economía, Fomento y Turismo, alineándose con los más altos estándares internacionales en protección de datos. Ante ello, no podemos si no manifestar nuestra preocupación cuando nuevamente se analiza la institucionalidad encargada de velar por el respeto de los derechos de los titulares de los datos personales como asimismo el cumplimiento normativo.

A continuación, entregamos observaciones preparadas por nuestra Mesa de Regulaciones Digitales, cuyo objetivo es robustecer el proyecto y contribuir al debate para una legislación que proteja eficazmente los derechos de las personas, permita el desarrollo de nuevos emprendimientos y armonice la propuesta a los más altos estándares regulatorios internacionales.

1. OBSERVACIONES AL CATÁLOGO DE DEFINICIONES (Artículo 2)

1.1. **Se sugiere la eliminación de definiciones dispositivas** (Artículo 2). Las definiciones son útiles para establecer con exactitud el alcance de las palabras usadas en una ley; y **sugerimos distanciarse de definiciones sustantivas**, esto es, establecer una prohibición, un requisito o una autorización en

sí mismas. Para eso está el cuerpo de la ley. Actuar de otro modo implica una reiteración de los mismos conceptos, o, peor aún, el riesgo de contradicción en un cuerpo legal.

Observamos que una buena cantidad de las definiciones del proyecto tienen este defecto. Tal es el caso de las "definiciones" de los derechos de los titulares – artículo 2 letras p) a t) – que no entregan una definición, sino que reitera (en algunos casos, de modo no idéntico) lo que en la parte dispositiva – artículos 4 y siguientes – ya está contenido. En este sentido, no se hace necesaria una definición que simplemente repite lo dispuesto más abajo.

- **Recomendación 1:** Eliminación de las definiciones dispositivas.

1.2. **Eliminación de "hábitos personales" en definición de datos sensibles** (Artículo 2 g). La definición de datos sensibles incluye un elemento ajeno a la regulación del Reglamento General de Protección de Datos de la Unión Europea (el "RGPD")[1]: los "hábitos personales". Los datos sensibles reciben una protección aumentada porque el legislador busca evitar que el tratamiento de cierto tipo de datos contribuya a una discriminación arbitraria del sujeto, y por ello protege especialmente datos personales que *revelen* elementos como la orientación sexual, la religión, la afiliación política, el origen étnico. Un hábito personal en sí mismo no constituye un dato sensible, pero puede llegar a constituirlo si éste revela alguno de los otros elementos clásicos de la definición. Del mismo modo, el registro de una conducta no debe considerarse sensible en sí mismo, pero si se debe tratar como sensible si revela la afiliación política; un hábito personal, esto es, la mera repetición de un acto en el tiempo sólo debería considerarse sensible si revela algún elemento sensible.

- **Recomendación 2:** Eliminación de la frase "hábitos personales" de la definición de dato sensible.
- *¿Tiene RGPD una norma similar a la del actual proyecto?* No. Nuestra recomendación sigue la línea del RGPD.

1.3. **Eliminación de definición de Motor de búsqueda** (Artículo 2 x). La frase "motor de búsqueda" únicamente se define, pero no se usa a lo largo de todo el proyecto de ley. Esta definición dispositiva entrega una interpretación particular sobre una definición más amplia y ya existente, que es la del responsable del tratamiento de datos. En la estructura de ésta y de todas las legislaciones de privacidad sofisticadas, una entidad que hace tratamiento de datos puede ser bien responsable, o bien encargado (mandatario); dependiendo de si decide o no directamente sobre los fines y medios del tratamiento.

Pareciera innecesario, entonces, que una ley se pronuncie sobre un solo tipo de "persona" para declarar algo tan específico como a si procede o no, respecto de ésta, el derecho de cancelación. Por último, los motores de búsqueda no son creadores de los datos ni los almacenan, solo facilitan

[1] "**Artículo 9 RGPD:** *Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida o las orientaciones sexuales de una persona física".*

el acceso a esos datos almacenados en otras fuentes, y los cambios tecnológicos podrían dejar rápidamente obsoleta la definición y tener consecuencias no deseadas.

- **Recomendación 3:** Eliminación de la definición de "motor de búsqueda".
- *¿Tiene RGPD una norma similar a la del actual proyecto?* No. Nuestra recomendación sigue la línea del RGPD.

1.4. **El concepto de "bloqueo" debe excluir el almacenamiento.** (Artículo 2 b) La regulación en torno al "bloqueo" de datos, de la forma en que lo plantea la actual Ley 19.628 y que perpetúa el Proyecto, es una innovación de la ley chilena. El RGPD no regula la institución del bloqueo. El Proyecto lo define como *la suspensión temporal* ***de cualquier operación de tratamiento*** *de los datos almacenados.* Esto es impracticable, pues cualquier operación de tratamiento de datos involucra necesariamente el almacenamiento. Luego, no es posible "suspender temporalmente" el almacenamiento sin eliminar el dato personal.

Sin perjuicio de este error en la definición que impide su aplicación práctica, la institución misma del bloqueo es artificial e innecesaria, y **no presenta un beneficio evidente para los titulares**:

- El bloqueo no es un derecho autónomo, sino que se presenta como una especie de "orden de no innovar" *accesoria a los derechos de rectificación, cancelación u oposición*, donde el titular puede solicitar la suspensión temporal de tratamiento de sus datos con efecto inmediato, otorgando un plazo de solo 2 días para responder a la solicitud de bloqueo.
- El bloqueo, de mantenerse, debería aplicarse únicamente para los derechos de cancelación u oposición, pues no hace sentido una garantía tan onerosa de implementar para un escenario donde el titular únicamente desea rectificar, y no eliminar un dato.
- El bloqueo debería ser aplicable únicamente para los escenarios donde la base de legalidad del tratamiento es el consentimiento; de otro modo, un titular podría solicitar la eliminación de un dato que el responsable debe procesar (por ejemplo) por obligación legal o por interés legítimo; donde una solicitud de rectificación, cancelación o bloqueo sería necesariamente rechazada.
- El incumplimiento de las obligaciones de bloqueo se tarifica por el Proyecto como una infracción grave, lo que lleva a aparejado una multa de mínimo 101 UTM.

- **Recomendación 4:** Eliminación de la institución del bloqueo en los artículos 11, 23, 34ter f) y 34 quater i). En subsidio, (i) modificar la definición para excluir expresamente el almacenamiento"; (ii) supeditarla a los escenarios donde la base de legalidad es el consentimiento; y (iii) aumentar el plazo para atender la solicitud de bloqueo; (iii) no calificarlo como infracción grave.
- *¿Tiene RGPD una norma similar a la del actual proyecto?* No

2. LIMITACIÓN EN EL DERECHO DE RECTIFICACIÓN (Art. 6)

El Proyecto obliga al responsable que recibe una solicitud de rectificación, a "comunicar los datos rectificados" a las entidades a las que hubiera **comunicado** (de responsable a mandatario) **o cedido** (de responsable a responsable) los datos.

Puede entenderse que un responsable deba asegurarse que los datos sean íntegramente rectificados dentro de su esfera de control, y que por ese motivo deba ordenar a sus encargados o mandatarios (a quienes le *comunicó* los datos) que lleven a cabo la rectificación. La obligación deviene en desproporcionada, sin embargo, si se entrega a un responsable la carga de comunicar "datos rectificados" a entidades cesionarias de los datos que son, a su turno responsables directos de ellos. Las obligaciones del Proyecto relativas a la cesión son estrictas e involucran el conocimiento del titular a las que los datos se hayan cedido es desproporcionada e innecesaria. Esta comunicación se hace impracticable, por ejemplo, para una entidad que constantemente comunica y realiza rectificaciones de datos.

- **Recomendación 5:** Eliminar el vocablo cedido del párrafo segundo del artículo 6
- *¿Tiene RGPD una norma similar a la del actual proyecto?* No, pues el RGPD dispone en su artículo 19 que dicha comunicación se realizará "salvo que sea imposible o exija un esfuerzo desproporcionado. Nuestra recomendación sigue la línea del RGPD.

3. TRATAMIENTO AUTOMATIZADO DE DATOS (Art. 8 y Art. 15 ter)

El tratamiento automatizado de datos y la elaboración de perfiles se regula en forma de un nuevo derecho de oposición a las valoraciones personales automatizadas, y ciertas restricciones al tratamiento automatizado de grandes volúmenes de datos.

3.1. **Regulación anti discriminación en sede de privacidad.** Esta regulación busca evitar los sesgos algorítmicos y la afectación de derechos del titular, derivada de la toma de decisiones automatizadas. El elemento subyacente en estas restricciones es la no discriminación. En ese sentido, pareciera que la sede para regular los riesgos relacionados con los sesgos algorítmicos debería estar más en la esfera de legislaciones anti discriminación, que en la de una regulación de cumplimiento técnico como es la protección de datos. Nos parece relevante regular esta materia generando obligaciones de transparencia, de mitigación de riesgos de sesgo algorítmico y de incentivo a evaluaciones de impacto algorítmico (del modo en que plantea, por ejemplo, el *Algorithmic Accountability Act de 2022*[2]), pero tenemos dudas si la sede de protección de datos es la más adecuada para ello.

[2] Wyden, Booker and Clarke; disponible en https://www.wyden.senate.gov/news/press-releases/wyden-booker-and-clarke-introduce-algorithmic-accountability-act-of-2022-to-require-new-transparency-and-accountability-for-automated-decision-systems

- **Recomendación 6:** Regular los efectos anti discriminatorios del tratamiento automatizado de todo tipo de datos en un cuerpo legal diferente.
- *¿Tiene RGPD una norma similar a la del actual proyecto?* sí

3.2. **Se regula únicamente el ámbito automatizado, como si el tratamiento no automatizado fuera menos falible.** La regulación va en la línea de proscribir eventuales actos discriminatorios relacionados con decisiones donde no interviene un ser humano, como si pudiéramos presumir un mayor grado de ecuanimidad en el involucramiento humano. Dado que el tratamiento de datos ocurre tanto en ambientes automatizados y no automatizados, esta regulación se hace cargo indirectamente de los efectos discriminatorios únicamente en uno de esos dos ámbitos, el automatizado.

3.3. **El ámbito de decisiones "que le conciernen" al titular es innecesariamente amplio.** El derecho de oposición del artículo 8 bis surge respecto de "*decisiones que le conciernan*" al titular, en tanto esas decisiones estén basadas en un tratamiento automatizado de datos. Una decisión puede concernirle al titular sin tener ninguna importancia, pero con afectación en sus derechos. El RGPD en cambio, en la norma similar de su artículo 22.1,[3] introduce un criterio de relevancia, señalando que el derecho existe cuando la decisión "*produzca efectos jurídicos en él* ***o le afecte significativamente*** *de modo similar*".

- **Recomendación 7:** Seguir la línea de RGPD, introducir el concepto de decisiones que le afecten significativamente, en lugar de la referencia a las "decisiones que le conciernan".
- *¿Tiene RGPD una norma similar a la del actual proyecto?* No. Nuestra recomendación sigue la línea del RGPD.

4. REQUISITOS Y PLAZO PARA ATENDER DERECHOS ARCO (Art. 11)

4.1. **Cálculo del plazo para atender el ejercicio de derechos ARCO.** El artículo 11 detalla los elementos que debe contener una solicitud de ejercicio de derechos ARCO, es decir, qué información debe entregar el titular al responsable cuando ejerce alguno de sus derechos de acceso, rectificación o cancelación. El primero de ellos requiere que, junto con la individualización del titular, éste debe acompañar la "*autenticación de su identidad de acuerdo con los procedimientos, formas y modalidades que establezca la Agencia*". Esto es adecuado y necesario para proteger los derechos de los titulares, evitando un escenario donde alguien, apersonando al verdadero titular, solicite y obtenga información de un tercero. En Europa han ocurrido y se han sancionado brechas de seguridad derivadas de la insuficiente autenticación de un usuario que pretende ejercer un derecho ARCO sin ser el verdadero titular.

[3] Artículo 22.1 RGPD: 1. *Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.*

Al ser el deber de autenticación indispensable para atender el derecho ARCO; el plazo para responder al ejercicio del derecho debería empezar a correr solo desde que el titular satisface adecuadamente el requisito de la autenticación.

4.2. **Extensión del plazo para atender el ejercicio de derechos ARCO.** El Proyecto de ley establece un plazo de 15 días hábiles (3 semanas) para pronunciarse sobre la solicitud. Este plazo es breve para escenarios de tratamientos complejos o donde los datos personales son difíciles técnicamente de aislar. RGPD establece una obligación de responder "sin dilaciones indebidas" y en un plazo máximo de un mes[4], lo que introduce un elemento de racionalidad y proporcionalidad al cumplimiento de la obligación, la que en ciertos casos podrá ser mucho más breve, y en otros de tratamientos más complejos, debería necesariamente ser más extenso; pero nunca superando un mes.

- **Recomendación 8:** (i) Modificar el inciso segundo del artículo 11 considerando un plazo mayor para atender los derechos ARCO y (ii) asociar el comienzo del plazo al cumplimiento de los elementos del inciso primero del artículo 11, es decir, que no pueda correr el plazo si no se ha podido verificar la identidad del solicitante.
- *¿Tiene RGPD una norma similar a la del actual proyecto?* No. Nuestra recomendación sigue la línea del RGPD.

4.3. **Requisitos de autenticación a determinar por la Agencia.** El artículo 11 letra a) señala que los requisitos de autenticación de la identidad del titular se determinarán "*de acuerdo con los procedimientos, formas y modalidades que establezca la Agencia*.". Esta redacción significará que mientras la Agencia no emita un pronunciamiento sobre tales requisitos técnicos, los responsables no podrán solicitar la autenticación o correcta individualización de los titulares; lo que contradice sus propias obligaciones de seguridad. Luego, debería establecerse la facultad de solicitar información de autenticación en forma autónoma, y a renglón seguido establecerse que la Autoridad "podrá" determinar los procedimientos, formas y modalidades de tal autenticación.

- **Recomendación 9:** Modificar la letra a) del Artículo 11 para *permitir* que la Agencia pormenorice los procedimientos, formas y modalidades de la autenticación de identidad, pero que, en ausencia de tal guía, sea evidente que se mantiene el requisito de autenticación.
- *¿Tiene RGPD una norma similar a la del actual proyecto?* No. Nuestra recomendación sigue la línea del RGPD.

[4] Considerando 59 RGPD: *El responsable del tratamiento debe estar obligado a responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas.*

5. CUANDO SE PUEDE ACUDIR AL INTERÉS LEGÍTIMO (ART. 13)

El Proyecto, al tratar el interés legítimo como base de licitud, señala que es aplicable cuando el tratamiento es necesario para la satisfacción de un interés legítimo, pero *siempre que con ello no se afecten los derechos y libertades del titular*. El responsable, por lo tanto, debe cotejar su interés legítimo con los derechos del titular, y en esta evaluación, los derechos del titular no pueden resultar afectados. Esta referencia debiese ser más precisa, tal como lo establece el considerando número 47 del RGPD[5], que modera la referencia a los "intereses o derechos y libertades del interesado (titular)" señalando que debe tenerse en cuenta las "expectativas razonables de los interesados basadas en su relación con el responsable [del tratamiento]"; y que en vez de hablar de "afectar" los derechos y libertades del titular, escoge la palabra "prevalecer"; lo que permite un test práctico y más fácil de resolver. La diferencia entre afectar un derecho (como en el Proyecto), o el que el derecho prevalezca no es menor, pues una afección menor y poco relevante sigue siendo una afección, lo que impediría que en la práctica pueda utilizarse esta base de legalidad que ha provisto a Europa de una flexibilidad tremendamente útil. El uso del concepto "prevalecer" refleja la naturaleza de esta base de licitud, que exige hacer un juicio de proporcionalidad o prueba de balance entre los intereses del controlador y los del titular, lo que no se desprende con tanta facilidad del concepto de "afectación", que es el que emplea el Proyecto actualmente.

- **Recomendación 10:** Recoger en el artículo 13 e) el elemento de intereses legítimos que no prevalecen sobre los derechos de los titulares, en reemplazo del vocablo "no se afecten".
- *¿Tiene RGPD una norma similar a la del actual proyecto?* No. Nuestra recomendación sigue la línea del RGPD.

6. OBSERVACIONES A LA OBLIGACIÓN DE NOTIFICAR BRECHAS DE SEGURIDAD (Art. 14 sexies)

6.1. **Obligación directa del encargado de notificar brechas de seguridad.** La obligación de notificación de brechas de seguridad es uno de los pilares de un ecosistema sano de ciberseguridad. Para ello, nacen obligaciones del responsable de la base de datos de notificar a cierta autoridad la ocurrencia de brechas de seguridad, cuando las brechas tienen ciertas características que, por su gravedad, la hacen digna de aviso.

El Proyecto de ley es completamente innovador al determinar quiénes están obligados a notificar, pues en lugar de generar esta obligación únicamente en el responsable, extiende la obligación al encargado o mandatario para el tratamiento de los datos. El RGPD en su artículo 33.2 obliga a notificar brechas únicamente al responsable, y obliga al encargado a notificar "*sin dilación indebida*" a su responsable, para que sea el responsable quien haga la calificación de si la brecha es o no notificable, a quien notificar, en qué momentos y respecto de qué información.

[5] https://gdpr-text.com/es/read/recital-47/#:~:text=(47)%20El%20inter%C3%A9s%20leg%C3%ADtimo%20de,interesado%2C%20teniendo%20en%20cuenta%20las

Como el encargado trata los datos en representación del responsable, a través de la ficción jurídica de la representación, el tratamiento del encargado es en realidad el tratamiento del responsable. Por ese motivo se justifica que la relación jurídica entre el responsable y el encargado esté regulada, y que el responsable, al final del día, tenga responsabilidad sobre el tratamiento del encargado, cuando éste se efectúa dentro de los límites del encargo.

Observamos un problema práctico importante en esta innovación, que surge, en nuestra opinión, de un desconocimiento de la anatomía de un incidente de seguridad. Si tanto responsable como encargado deben notificar a la autoridad, o en ciertos casos incluso a los titulares, **de la misma brecha**, lo que inevitablemente sucederá es que:

- Los notificados (autoridad o titulares) recibirán una notificación doble por el mismo hecho.
- Se generarán calificaciones de brechas notificables disímiles. Dado que se debe notificar las vulneraciones "*que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita … o la comunicación o acceso no autorizados …, cuando exista un riesgo razonable para los derechos y libertades de los titulares*", podrán responsable y encargado tener opiniones diferentes de la existencia de este riesgo razonable para los titulares. Luego, bien podría suceder que un procesador prefiera notificar una brecha menor[6] que el responsable de datos, su mandante, califique de no notificable.
- El encargado, con una gran frecuencia, no solo no conoce el contenido de la información que le es encargada tratar, sino que no la quiere ni debe conocer. Es deseable, de hecho, que un prestador de servicios de almacenamiento, por ejemplo, no tenga un acceso real o sencillo al contenido específico de la información; o que las herramientas para desencriptar información almacenada por un proveedor externo no estén en poder de tal proveedor. De este modo, la obligación del proveedor de notificar una brecha a la autoridad, o aún más, a los titulares directamente, deviene en imposible, pues para hacerlo debe estar en posición de poder siempre conocer los tipos de datos y la identificación de cada uno de los titulares de aquellos. La gestión de bases de datos en el siglo XXI no funciona de manera tan simple como para poder exigir de encargado la identificación de datos sensibles, datos de menores o datos económicos y la notificación directa del procesador al titular.

En este sentido, la norma debería considerar que el encargado cumple un rol técnico y, por definición, neutro.

- **Recomendación 11:** Eliminar en el artículo 14 sexies las referencias al encargado.

  Generar un nuevo inciso en el artículo 15 bis, que señale una obligación similar a la del artículo 33.2 de RGPD, requiriendo que el encargado notifique "sin dilación indebida" al responsable.

  Eliminar del inciso cuarto del artículo 15 bis la referencia al artículo 14 sexies.

- *¿Tiene RGPD una norma similar a la del actual proyecto?* No. Nuestra recomendación sigue la línea del RGPD.

[6] "S*e cayó el pendrive al suelo"* es un ejemplo usado con frecuencia para explicar que en el día a día existen una infinidad de riesgos menores que no justifican el costo de recursos públicos y privados en un esfuerzo de notificaciones de brechas.

6.2. **Notificación directa de brechas de seguridad a los titulares.** El Proyecto genera en el artículo 14 sexies una obligación de notificación directa a los titulares que está **calificada únicamente por el contenido de los datos vulnerados**. Luego, para que deba notificarse directamente a los titulares, basta que las vulneraciones se refieran a datos sensibles, de menores de 14 años o económicos; sin importar el riesgo involucrado en tal vulneración. El RGPD, reconociendo la carga involucrada en una notificación de brecha masiva a los titulares, sujeta esta obligación en su artículo 34 únicamente si la probable violación entraña "*un alto riesgo para los derechos y libertades*" de los titulares.

Adicionalmente, el RGPD genera excepciones a esta obligación de notificación directa, de las cuales el Proyecto únicamente recoge la de esfuerzo desproporcionado en la notificación; pero no incluye las del artículo 32.3 letras a) y b), esto es, escenarios donde se han aplicado medidas de seguridad robustas a los datos afectados por la violación, como el cifrado; o cuando se hayan tomado medidas que garanticen que ya no existe la probabilidad de este alto riesgo para los derechos del titular.

- **Recomendación 12:** Modificar el artículo 14 sexies inciso tercero, para incluir (i) el concepto de alto riesgo para los derechos y libertades del titular derivado de la violación, como un elemento determinante para la notificación directa a los titulares (ii) excepciones a la obligación a notificar directamente a los titulares en la misma línea que el RGPD artículo 32.3 letras a) y b), y (iii) la prohibición de identificar en concreto los datos objeto de la brecha cuando la notificación se hace por medios públicos.
- *¿Tiene RGPD una norma similar a la del actual proyecto?* No. Nuestra recomendación sigue la línea del RGPD.

7. INSUFICIENTES INCENTIVOS EN LA ADOPCIÓN DE MODELOS DE PREVENCIÓN DE INFRACCIONES (Art. 34 quater y Art. 51)

Los modelos de prevención entregan herramientas a los regulados para facilitar el cumplimiento regulatorio, pero también, y muy especialmente, para incentivarlo. Si los incentivos no están bien estructurados, la regulación de un modelo de prevención de infracciones puede perder toda su efectividad. El texto actual del Proyecto, lamentablemente, tiene hoy ese vicio.

7.1. **Sanción gravísima por un error en el proceso de certificación** (34 quater J)**.** Un error que puede ser menor en el proceso de certificación trae aparejada una sanción desproporcionadamente alta. Se califica como infracción gravísima "*entregar información falsa, incompleta o manifiestamente errónea en el proceso de registro o certificación del modelo de prevención de infracciones*". Es decir, si en el proceso de registro del modelo de prevención de infracciones se omite un documento y la información es incompleta, la sanción asociada a la infracción es gravísima, cuya sanción mínima es de aproximadamente $278 millones (5.001 UTM); y máxima aproximadamente $550 millones (10.000 UTM).

Esta infracción es la única de las gravísimas no asociada a malicia o culpa grave.

7.2. **Reporte obligatorio** (artículo 51 (c) iv). El programa de cumplimiento, obligatoriamente, debe establecer "*mecanismos de reporte hacia las autoridades para el caso de contravenir lo dispuesto en la presente ley*". Un mecanismo de reporte interno de incumplimientos es eficiente y aumenta la concientización de los trabajadores, pero la institucionalización de una obligación de denuncia a las autoridades —es decir, **generar una obligación de los trabajadores de reportar cualquier infracción** a la ley de protección de datos cometida por la empresa o por sus compañeros de trabajo— es un desincentivo gigantesco a la adopción del programa de cumplimiento; sin mencionar que caben dudas respecto a su constitucionalidad.

7.3. **La estructura de la regulación es confusa** (artículos 48 y 49). Se establece una conducta obligatoria general de adoptar acciones para prevenir infracciones (art 48) y una conducta voluntaria específica de adoptar un modelo de prevención de infracciones (art 49). Seguidamente, la ley entiende que se configura un modelo de prevención de infracciones —que, recordemos, es voluntario— con la implementación de cualquiera de estas dos acciones: (1) la designación de un "encargado de prevención" o (2) la adopción de un programa de cumplimiento. Extrañamente, entre los elementos mínimos del programa de cumplimiento está la designación de un encargado de prevención —el que en sí mismo es también un modelo de prevención de infracciones.

7.4. **El incentivo es escaso.** El incentivo para que una empresa adopte un modelo de prevención de infracciones está en la configuración de una circunstancia atenuante: en caso de infracción, su culpa puede ser calificada con menor severidad. En el Proyecto, el art 36 N° 5 considera como una circunstancia atenuante "*el haber cumplido diligentemente sus deberes de dirección y supervisión para la protección de los datos personales sujetos a tratamiento, lo que se verificará con el certificado expedido de acuerdo con lo dispuesto en el artículo 52*".

¿Cuál es este certificado que permite obtener la atenuante? Bajo el artículo 52, son objeto de certificación los modelos de prevención de infracciones y los programas de cumplimiento. Como un modelo de prevención de infracciones puede suponer tanto la designación de un delegado de protección de datos como la adopción de un programa de cumplimiento, se debe entender entonces que la sola designación del delegado puede ser objeto de certificación. Dicho de otro modo, "lo certificado" no es únicamente el programa de cumplimiento, sino también la otra modalidad de modelo de prevención de infracciones, que es el establecimiento de este delegado de protección de datos. No queda claro, entonces, cómo una designación puede ser objeto de certificación y tener el mismo valor que el establecimiento de un programa, el que tiene muchos más requisitos.

- **Recomendación 13:** (i) Asociar los programas de prevención de infracciones a estímulos concretos, como la exoneración de responsabilidad (sujeto a supuestos de gravedad y proporcionalidad) para aquellos responsables del tratamiento de datos que decidan optar por la implementación de modelos de prevención (ii) Eliminar la referencia al modelo de prevención en el catálogo de infracciones gravísimas (34 quater j); y (iii) Eliminar el requisito de un programa de prevención de contemplar un mecanismo de reporte obligatorio de los trabajadores a la autoridad, en el artículo 51 (c) iv).
- *¿Tiene RGPD una norma similar a la del actual proyecto?* No

8. LA INSTITUCIÓN DE CESIÓN DE DATOS PERSONALES ES INNECESARIA Y REDUNDANTE (Artículo 15)

La institución cesión de datos es una innovación del Proyecto de ley. El RGPD no contempla una regulación específica sobre cesión de datos.

El traspaso de datos de responsable a responsable, qué duda cabe, debe ser objeto de restricciones de principios y bases de legalidad; y para ello el Proyecto ya regula un estatuto estricto de bases de legalidad y principios. La consideración de la cesión de datos como un estatuto paralelo con sus propias bases de legalidad, y el hecho que el inciso cuarto del artículo 15 les haga aplicables las normas del contrato de cesión hacen presumir que, por lo menos respecto de la cesión, el legislador entiende que los datos personales son bienes económicos apropiables, que pueden pasar de un patrimonio a otro con el cumplimiento de ciertos requisitos, que pueden ser objeto de tradición como lo sería un mueble o las acciones de una sociedad.

Por ello, creemos que no es conveniente crear una fuente de licitud específica para la cesión, debiendo remitirse a las bases de licitud de cualquier tratamiento de datos (art. 13 letra c) del proyecto de ley), manteniendo las limitaciones asociadas a la exigencia de mecanismos de seguridad para evitar la vulneración de los datos cedidos.

- **Recomendación 14:** Eliminar el artículo 15
- *¿Tiene RGPD una norma similar a la del actual proyecto?* No

9. OBSERVACIONES AL ESTATUTO DE SANCIONES (Art. 35)

9.1. **Montos mínimos de sanciones.** Para darle un mayor grado de razonabilidad a la norma, recomendamos que no se establezcan montos mínimos de multa, en coherencia con la estructura adoptada por el RGPD; que tarifica las infracciones, pero las asocia a sanciones de multas con un máximo, pero no un mínimo. Eso permitirá además que la autoridad de protección de datos tenga mayor libertad en la aplicación de sanciones, sin tener que estar obligada a una multa mínima en casos de infracciones graves y gravísimas. Las microempresas y las empresas pequeñas y medianas que cometan infracciones graves o gravísimas difícilmente podrán pagar las multas que la norma actual establece como mínimos para cada nivel de gravedad. Si una pyme no actualizó a tiempo su política de privacidad, o si el método de recogida de consentimiento resulta ser errado, su accionar deberá ser sancionado como infracción grave del artículo 34ter a); y por lo tanto la multa mínima será necesariamente de 101 UTM.

En la práctica, la ausencia de un “piso” en las multas beneficiará el nivel de aplicación real de la Ley en nuestro país, y la progresividad con que la Autoridad pueda empezar a aplicar la ley.

9.2. **Multas asociadas a los ingresos.** Se ha discutido por los señores diputados en relación con la determinación de las multas considerando un porcentaje sobre los ingresos del infractor en el año inmediatamente anterior, en línea con lo dispuesto por el RGPD y a su vez tomando como ejemplo la normativa de libre competencia DL 211 de 1973. Al respecto, cabe tener presente la cultura y

trayectoria que como país tenemos en protección de datos, la cual dista considerablemente de los más de 70 años de Europa, quienes han transitado y evolucionado paulatinamente hasta el exigente estándar que contempla el RGPD y el monto de las multas. Misma experiencia es aplicable respecto de la regulación nacional de libre competencia.

Finalmente, se sugiere considerar el tamaño de la empresa disponiendo que las sanciones pecuniarias a pymes solo se impondrán cuando la infracción se cometió de forma dolosa o con negligencia grave.

- **Recomendación 15:** Eliminar los montos mínimos de las multas y considerar el tamaño de la empresa como un elemento a considerar en la determinación del monto de la multa que corresponda aplicar, introduciendo los conceptos de dolo o negligencia grave.
- *¿Tiene RGPD una norma similar a la del actual proyecto?* No. Nuestra recomendación sigue la línea del RGPD.

9.3. **Suspensión de actividades de tratamiento (Art. 38).** En concordancia con lo señalado en numeral 1.4. anterior, respecto del bloqueo, la suspensión del tratamiento es en la práctica imposible de cumplir, en particular considerando que el almacenamiento es una forma de tratamiento.

Por otro lado, esta sanción es extremadamente gravosa y desproporcionada para los responsables de datos, pues su aplicación práctica bien puede significar la paralización total de empresas de distintos rubros, siendo la ciudadanía la más afectada.

Finalmente, los elevados montos incorporados en el catálogo de sanciones del Proyecto, se ven incrementados en casos de reincidencia. Así, el Proyecto dispone que la Agencia podrá aplicar una multa de hasta tres veces el monto contemplado para la infracción cometida, actuando como desincentivo y sanción suficiente para aquellos responsables que cometan infracciones reiteradas.

- **Recomendación 16:** Eliminar la sanción de suspensión de actividades de tratamiento
- *¿Tiene RGPD una norma similar a la del actual proyecto?* No. Nuestra recomendación sigue la línea del RGPD.