Minuta presentación Comisión Mixta Proyecto de Ley N°12.409-03 ("PL Pro Consumidor")

Jessica Matus Arenas[1]

19 de mayo de 2021

1. La necesidad de una agencia independiente y especializada en materia de protección de datos personales

1.1. El contexto actual de masificación de internet y la disrupción de las tecnologías digitales con el consiguiente flujo de información representa un desafío para la ética, normas y derechos fundamentales en formas nunca antes vistas, como ocurre con el derecho a la privacidad y a la protección de los datos de las personas.

1.2. Existen diversos actores e intereses involucrados en la economía digital basada en el flujo masivo de datos razón por la cual el rol de una autoridad de protección de datos ("APD") independiente resulta clave para proteger los derechos y libertades de los titulares. Sólo mediante el establecimiento de una **autoridad independiente y especializada**, que lleve a cabo sus tareas de manera libre de influencias externas, incluyendo al gobierno de turno, será posible garantizar la eficacia y fiabilidad de la supervisión y fiscalización.

1.3. La existencia de una **independencia política, funcional y presupuestaria** de la autoridad de control se vuelve crucial no solo en relación con el ámbito privado, sino también con el grado de control que pueda tener sobre el sector público, pues las APD también deben fiscalizar instituciones públicas, considerando que el Estado es uno de los responsables de tratamiento de datos personales más importantes en cada país. De lo contrario el fiscalizador tiene interés directo en no reportar las conductas del fiscalizado, existiendo un incentivo para aplicar un criterio parcial y potencialmente vulnerando garantías fundamentales.

1.4. Como muestra a nivel local, podemos recordar el tratamiento ilícito de datos personales que hizo el Ministerio de Educación el año 2019 mediante el envío de masivo de correos electrónicos **con** información relativa al proyecto de ley "Admisión Justa", fin completamente distinto para el cual habían sido recolectados los datos, que da cuenta de la necesidad de independencia política.

1.5. Además de independientes, las APD deben ser instituciones altamente especializadas, pues el dominio requerido no es sólo normativo, sino también técnico y que requiere una formación en constante desarrollo, dado que los mayores riesgos a la privacidad y a la protección de datos, derivan del incesante avance de tecnologías con altos grados de disrupción: marketing digital, herramientas de perfilamiento, IoT, *big data*, IA, televigilancia, biometría, *fintech*, etc. Como por ejemplo evaluar cuándo una respuesta ante incidentes/brechas de seguridad es la adecuada, a que se refiere este proyecto.

[1] Abogada Universidad de Chile, Diplomada en Derecho Informático, especialista en protección de datos personales. Directora de Tecnologías de FerradaNehme; presidenta del Capítulo chileno de Internet Society y fundadora de Datos Protegidos.

1.6. La importancia de contar con una agencia fuerte, robusta e independiente es relevante no sólo a nivel local sino que también internacional ya que la tendencia es hacia el fortalecimiento de la institucionalidad en materia de protección de datos. Prueba de lo anterior, fue el pronunciamiento en 2020 del Caso de Schrems del Tribunal de Justicia de la Unión Europea, que reconoció la capacidad de las autoridades de control de suspender cualquier transferencia de datos transfronteriza cuando el Estado destinatario (en este caso EEUU, a través de Facebook), no satisfagan un estándar adecuado de protección. (Puerto, M. y Sferrazza, P. (2017).

2. La necesaria consistencia entre el PL Pro Consumidor y el Proyecto de Ley de Datos Personales

2.1. Es necesario recordar que en materia de protección de datos personales actualmente se encuentra en tramitación en el Congreso Nacional un proyecto de ley (boletines N°11.144-07 y N°12.092-07, "Proyecto de Ley de Datos Personales"), que viene a adecuar la regulación chilena en materia de protección de datos personales a los estándares internacionales vigentes, en particular, de la OCDE y de la Unión Europea (expresados en el Reglamento General de Protección de Datos o GDPR, por sus siglas en inglés), modificando casi en su totalidad a la actual ley de protección de datos (Ley N°19.628, de Protección de la Vida Privada, "LPD"), que data de 1999.

2.2 En concordancia con esos estándares internacionales, el Proyecto de Ley de Datos Personales, tiene como uno de sus pilares la creación de una APD, encargada de (1) fiscalizar y velar por el cumplimiento de la normativa aplicable en materia de protección de datos; (2) aplicar, interpretar administrativamente y dictar instrucciones generales relativas a dichas normas; (3) resolver las solicitudes y reclamaciones que formulen los titulares en contra de los responsables de datos; (4) investigar, determinar las infracciones en que incurran los responsables de datos y aplicar las sanciones respectivas; (5) adoptar las medidas preventivas o correctivas; (6) proponer al Ejecutivo o al Congreso Nacional la dictación, modificación o derogación de determinadas normas; (7) desarrollar programas de difusión, educación e información en materia de protección de datos; (8) certificar, registrar y supervisar los modelos de prevención de infracciones y los programas de cumplimiento en el marco de la LPD; y (9) prestar asistencia técnica y colaborar con órganos públicos, entre otras.

2.3 Entonces, existirá prontamente – entendiendo que el Proyecto de Ley de Datos Personales concluirá su tramitación legislativa en un plazo razonable – una APD especializada (según el texto actual del Proyecto de Ley de Datos Personales, será el Consejo para la Transparencia quien tome este rol, dada su experiencia en materia de tratamiento de información, pasando a llamarse "Consejo para la Transparencia y Protección de Datos Personales"). Sin embargo, el presente proyecto de ley "Pro-Consumidor" entre su diversidad de normas que modifican la Ley N°19.496, de Protección de los Derechos de los Consumidores ("LPC") busca incorporar un artículo que facultaría al SERNAC a ejercer sus potestades en materia de protección de datos, tal como lo hace en materia de consumo.

Dichas potestades del SERNAC incluyen (1) amplias facultades de fiscalización; (2) interpretación administrativa de las normas de su ámbito de aplicación; (3) velar por el cumplimiento de dichas normas, lo cual incluye el iniciar o hacerse parte de acciones judiciales para la protección del interés individual, colectivo o difuso de los consumidores; (4) proponer al Ejecutivo la dictación, modificación o derogación de determinadas normas; (5) ejecutar programas de información y educación al consumidor, y elaborar y difundir información en pro de los consumidores; (6) realizar y promover estudios; (7) aprobar planes de cumplimiento en materia de protección del consumidor; y (8) llevar a cabo procedimientos voluntarios para la protección del interés colectivo o difuso de los consumidores (Procedimientos Voluntarios Colectivos, "PVC"), entre otras.

2.4 Se observa claramente que existen una serie de facultades del SERNAC que se superponen con aquellas que tendrá la APD. ¿Corresponde que un órgano especializado en materia de consumo se haga cargo de interpretar, fiscalizar, ejecutar, educar, ... en relación con normas de protección de datos? L**a existencia de una autoridad de control especializada en materia de protección de datos es uno de los puntos centrales para que la regulación de protección de datos de un país sea reconocida como adecuada por parte de organismos internacionales** – ¿Tiene sentido diluir las facultades y el poder de la APD, entregando gran parte de éstas al SERNAC?

2.5 La protección de los datos personales en Chile merece una APD fuerte, especializada, que pueda aplicar, fiscalizar y velar por el cumplimiento de la normativa que le compete. Y el SERNAC, cuya especialidad es otra, sin duda puede colaborar con la APD, complementarla en los aspectos que ésta no cubre. **En la práctica consagra un diseño institucional en protección de datos que no garantiza su carácter de derecho fundamental, imposibilitando una interacción óptima entre privacidad y otros ámbitos diversos como el derecho de consumo y la libre competencia que constituyen ejes de la economía digital". Estamos hablando de la explotación de datos de personas por las plataformas tecnológicas como fuente de poder de mercado que aumenta el riesgo de un ejercicio abusivo. Por último, hay que comprender que el derecho a la protección de datos es un derecho instrumental que permite el ejercicio de otros derechos, tales como la privacidad, la educación, la salud, la igualdad.**

3. La necesidad de la consagración de acciones colectivas en materias de datos personales

3.1 Existe una atribución en el PL Pro-Consumidor que no se encuentra regulada en el Proyecto de Ley de Datos Personales: la posibilidad de entablar acciones colectivas. Aun cuando a nivel internacional existe una clara tendencia a reconocer la importancia de este tipo de acciones, el actual Proyecto de Ley de Datos no se refiere al tema por lo que sería recomendable traer a la discusión su necesario reconocimiento y regulación. Para efectos de consistencia en la técnica legislativa, idealmente ambos proyectos de ley debieran estar alineados, es decir, por una parte el Proyecto de Ley de Datos Personales debiera consagrar la

existencia de acciones colectivas por infracción a la LPD a nivel general, especificando los requisitos para su procedencia y la naturaleza jurídica de las instituciones legitimadas para interponerlas, entre las cuales se encontrarían las señaladas en el artículo 51 de la LPC en una relación especie (consumo) dentro del género (datos personales); por otra, sería recomendable que el PL Pro Consumidor reconozca explícitamente dentro de la esfera de su competencia la interposición de acciones colectivas por interés colectivo o difuso en el contexto de una relación de consumo por infracción a la LPD. Con ello, se vería restringida la participación del SERNAC a la facultad de iniciar acciones colectivas en ámbitos de su competencia (en virtud del artículo 51) y sin por ello dejar fuera a otro tipo de relaciones en que podría existir un interés colectivo por una vulneración en materia de datos personales (como podría ocurrir por ejemplo, con infracciones dentro del contexto de una relación laboral).

3.2 Cabe destacar que el SERNAC ya tiene algo de experiencia en materia de interposición de acciones colectivas en materia de protección de datos, en el marco de cláusulas de contratos de adhesión que vulneraban los derechos de los consumidores en tanto titulares de datos personales: entre otras, en el año 2016 demandó colectivamente a COFISA (Tarjeta ABC Din), logrando que se declarara como abusiva una cláusula que autorizaba a la compañía a incluir a los deudores morosos en el boletín comercial (rol 4903-2015 de la Corte Suprema); y a Ticketmaster, donde se declaró como abusiva parte de la política de privacidad de su sitio web que autorizaba a la compañía a tratar sin restricciones los datos personales de las personas que visitaban la página (rol 1533-2015 de la Corte Suprema).

Sin embargo, la jurisprudencia en esta materia ha sido errática, pues los tribunales superiores de justicia, ante acciones colectivas del SERNAC por infracciones similares, han estimado en otras ocasiones que, en materia de protección de datos personales, no serían admisibles los juicios colectivos, por tratarse de "cuestiones esencialmente individuales", como señaló la Corte Suprema en el caso Ticketek (rol 26.932-2015 de la Corte Suprema).

3.3 Cabe señalar que, tanto la relación entre datos personales y derecho del consumo como la posibilidad de entablar acciones colectivas por infracciones a la LPD no ha sido un tema pacífico a nivel internacional y sigue siendo objeto de discusiones y reformas. El Reglamento General de Protección de Datos de la Unión Europea, cuerpo legal en el que se inspira nuestro Proyecto de Ley de Datos Personales, en su artículo 80, indica que las acciones de clase podrán ser presentadas por organismos sin fines de lucro dedicados a la protección de datos personales.

Esto ha sido implementado de diversas formas por los Estados Miembros. Por ejemplo, en Francia sólo tres tipos de asociaciones tienen la capacidad para presentar una demanda colectiva sobre datos: (1) asociaciones debidamente registradas por al menos cinco años, cuyo objeto social sea la protección de privacidad y datos personales; (2) representantes de asociaciones de consumidores a nivel nacional nivel y autorizados de acuerdo al Código de Consumo francés, cuando el procesamiento de datos en juego afecta a los consumidores; y (3) sindicatos de empleados o funcionarios representante en virtud del Código del Trabajo francés, cuando el tratamiento en juego afecte a los intereses de los individuos que los estatutos de estos las organizaciones les confían su defensa. En España, la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales no desarrolla el artículo 80 del GDPR. No obstante, es posible para las asociaciones de consumidores y usuarios defender los

derechos e intereses de sus miembros, la asociación en sí mismo, y el interés general de los consumidores y usuarios ante tribunales y jueces.

Conclusiones:

- Resulta sumamente relevante que Chile cuente con una APD independiente, especializada y con atribuciones suficientes que permitan la efectiva fiscalización de la gran variedad de actividades y partes interesadas que tratan datos personales.

- El PL en discusión restringe o reduce la protección de los datos a las relaciones de consumo, debilitando el necesario refuerzo a este derecho constitucional. Cede en favor del derecho de consumo, pero en detrimento de las garantías de protección de datos como derecho instrumental. Pareciera ser que es inocuo, pero las repercusiones son importantes en los derechos garantizados por la Constitución y la ley 19.628.

- No obstante, el PL Pro Consumidor sí recoge un punto que actualmente no está tratado en el Proyecto de Ley de Datos Personales: la necesidad de entablar acciones colectivas por infracciones en materias de datos personales de manera general y recogiendo el PL Pro Consumidor dicho mandato de manera específica, para que la interpretación de ambas normas sean interpretados de manera armónica.

- Por último, la naturaleza jurídica del SERNAC en cuanto autonomía e independencia, no cumple con los estándares de la UE en relación con la adecuación en materia de protección de datos.