Logrando el Equilibrio: Seguridad de Datos e Innovación en la Nueva Legislación

Cristián Oppliger[1]

El Proyecto de Ley de Protección de Datos Personales ha puesto sobre la mesa un importante desafío: cómo encontrar el justo equilibrio entre garantizar la seguridad de los datos y no obstaculizar el desarrollo e innovación de las empresas, especialmente las nuevas y pequeñas. Este es un punto fundamental, pues el mercado tecnológico avanza a un ritmo vertiginoso, y muchas empresas operan inicialmente como pymes, con pocos trabajadores y una limitada tracción comercial, pero -muchas veces estas mismas empresas- tienen una proyección tecnológica y comercial enorme. En este sentido, estas empresas de tecnología son parte integrante del mundo del capital de riesgo - venture capital -, por lo que tienen que estar de manera constante en procesos de levantamiento de capital y en análisis recurrentes en cuanto a su proyección comercial.

En el proyecto de ley se utiliza terminología legal amplia, como "estado de la técnica" o "tratamiento adecuado", lo que brinda cierta flexibilidad para realizar ajustes a medida en cuanto al tamaño de la empresa. En este sentido hay “estado de la técnica” y “tratamiento” por distintos tipo de industrias, por ejemplo, en la industria Fintech hay un “estado de la técnica” en cuanto a sus necesidades específicas de velocidad de procesamiento y respuesta “onsite” que puede ser muy distinto de otras industrias, como por ejemplo salud, donde se requiere analizar la información de forma detallada y donde puede haber un mayor lapso en cuanto al análisis cuantitativo. Sin embargo, es necesario que, en la determinación específica sobre su aplicabilidad, se utilicen y apliquen otras terminologías complementarias que definan el "estándar del mercado" -término utilizado ampliamente acá de forma intencional- actual, dada la velocidad de evolución tecnológica mencionada anteriormente. En relación con esto, surgen las siguientes interrogantes: en su aplicación concreta, ¿estas terminologías se definirán conforme a la realidad local chilena? ¿Tendrán en cuenta la rápida evolución tecnológica y las capacidades emergentes en cuanto a proyección, o se quedarán estancadas en un marco obsoleto antes de implementarse, generando

[1] Legal Lead Global66

así una fricción y costos que pueden ser innecesarios? ¿Cómo afectará la indefinición de estos conceptos en la proyección comercial de estas empresas?

Respecto al fondo del asunto, el principio de seguridad, de cumplimiento previo al tratamiento de datos, es crucial, especialmente durante el período de adecuación que la misma ley incorporará para su pleno cumplimiento. Sin embargo, quedan dudas conceptuales respecto a la terminología del proyecto de ley y las prácticas en cuanto a su aplicación. ¿Qué constituye un "tratamiento adecuado" desde el punto de vista de la seguridad? ¿Cómo se aplicará este enfoque de proporcionalidad según el tamaño y los recursos de cada organización? En este sentido la Agencia de Protección de Datos Española establece un estándar ISO a aplicar en esta materia en conjunto con una guía de gestión del riesgo y evaluación de impacto como ejemplos y estándares que darían lineamientos para el cumplimiento íntegro de lo anterior. La falta de claridad, reitero, en cuanto a una aplicación previa para cumplir con un estándar definido a implementar, podría traducirse en sobrecostos innecesarios, especialmente para startups y empresas de menor tamaño.

Otro aspecto clave es la gestión de brechas de seguridad y la notificación a los usuarios afectados. Si bien es comprensible la necesidad de transparencia, también hay que considerar la proporcionalidad y evitar generar alarmas injustificadas que podrían dañar la reputación de las empresas de manera desproporcionada en cuanto a la consideración misma de la brecha o ataque de seguridad. En este sentido, y solo para agregar un par de puntos, ¿cómo va a ser el flujo entre la agencia de protección de datos -encargada de recibir las afectaciones de seguridad de datos personales- y la agencia nacional de ciberseguridad respecto a aquellos giros compartidos con el deber de informar afectaciones y así evitar topes entre ambos reguladores? ¿Cuáles van a ser las consideraciones de hecho - en la calificación misma del incidente - respecto a la naturaleza de una eventual pérdida, filtración, destrucción o daño accidental? ¿A qué se refiere el proyecto de ley cuando señala que la notificación es por los medios "más expeditos posibles" y "sin dilaciones"? Siguiendo con el ejemplo del regulador español, se establece un criterio de “proporcionalidad” en cuanto las brechas “puedan poner en riesgo los derechos y libertades de las personas físicas” así, hay un deber de información a la Agencia de Protección de Datos Española en un plazo de 72 horas.

Asimismo, si la brecha no constituye una afectación evidente a los derechos y libertades hay un deber de documentación lo que va a permitir a la autoridad verificar el cumplimiento efectivo de los controles adoptados.

Tomando en consideración todo lo anterior, si bien la protección de datos es un objetivo deseable y necesario en cuanto a nuestra cultura y legislación, es fundamental que la nueva normativa encuentre un punto intermedio que fomente la adopción de buenas prácticas sin asfixiar la innovación y la proyección tecnológica; esto para que podamos adoptar nuevas tecnologías con beneficios evidentes para los titulares en cuanto al uso de su información. Un enfoque equilibrado, con parámetros claros pero flexibles, sería lo ideal para proteger a los ciudadanos sin frenar el desarrollo económico y tecnológico del país. La clave estará en lograr un marco regulatorio que promueva la seguridad sin convertirse en una camisa de fuerza para la innovación.