

Autoregulación, mecanismo efectivo para el tratamiento de datos personales



• Rodrigo Medina

El tratamiento de datos personales es clave para el funcionamiento de las empresas. Habitualmente, se dice que el mayor valor de un cliente no está en aquello que ya ha adquirido, sino en lo que podría adquirir en el futuro. En este sentido, toma vital relevancia la identificación de los clientes, la segmentación, su fidelización y una comunicación eficiente. La utilización de datos no se limita a los clientes, ya que esto se puede extrapolar al análisis de proveedores, socios o empleados y a la prevención de fraudes internos o riesgos de cumplimiento en el ámbito de la responsabilidad penal de las personas jurídicas. Sin embargo, la recolección y tratamiento de datos debe considerar el respeto y protección a la vida privada de las personas y de sus datos personales, derecho consagrado en nuestra Constitución, y el cumplimiento de la normativa vigente que regula el tratamiento y protección de datos.

Chile, a fines del siglo pasado, fue uno de los países precursores en Latinoamérica en la creación de un marco regulatorio para la protección de datos personales, a través de la dictación de la Ley 19.628 sobre Protección de la Vida Privada del año 1999. Transcurridos 20 años desde su entrada en vigencia, es evidente que la legislación chilena debe modernizarse y adaptarse a los grandes avances tecnológicos producidos en el presente siglo, cumpliendo con estándares internacionales que exigen una institucionalidad más activa y un sistema sancionatorio que garantice una protección real de la privacidad y datos de las personas.

En este sentido, la Organización para la Cooperación y el Desarrollo Económicos, OCDE, ha recomendado a nuestro país actualizar su marco regulatorio cumpliendo con estándares globales. Ello, sumado a la entrada en vigencia de diferentes normas que regulan la materia a nivel internacional, como el Reglamento General de Protección de Datos, GDPR, de la Unión Europea, impulsó que el Gobierno haya presentado con fecha 15 de marzo de 2017 un proyecto de ley que regula la protección y el tratamiento de los datos personales, buscando así modificar la Ley 19.628.

Este proyecto de ley establece como regla general que el tratamiento de datos (consistente en cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, procesar, almacenar, comunicar, transmitir o utilizar de cualquier forma datos personales o conjuntos de datos personales) es legítimo cuando el titular otorgue su consentimiento para ello. Dicha norma se

fundamenta en el reconocimiento del derecho de propiedad sobre sus datos al titular y a la relación asimétrica existente entre éste y el responsable del tratamiento de datos, donde el segundo tiene una posición de privilegio que podría traducirse muchas veces en la existencia de abusos, muy parecido a la relación entre un prestador de bienes o servicios y los consumidores que se comprometen por medio de un contrato de adhesión.

A su vez, el proyecto de ley considera excepciones a esta regla general, o sea, permite el tratamiento de datos personales sin el consentimiento del titular en los casos contemplados expresamente en ella. Una de estas excepciones a la regla general del consentimiento del titular es el interés legítimo como fuente de licitud en el tratamiento de datos personales, por medio del cual se permite el tratamiento necesario para la satisfacción de intereses legítimos del responsable o de un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del titular.

En este aspecto es importante mencionar la existencia de dos conceptos. El primero es el responsable, donde ubicamos a las empresas, y se trata de toda persona natural o jurídica, pública o privada, que decide acerca de los fines y medios del tratamiento de datos personales, independiente de si los datos son tratados directamente por ella o a través de un tercero mandatario o encargado.

El segundo es qué se entiende por interés legítimo. Por tal, se considerarían las actividades de prevención de fraude, seguridad de redes informáticas, tratamiento de datos realizado exclusivamente con fines históricos, estadísticos, científicos y de estudios o investigaciones, reporte de actividades criminales a las autoridades competentes y marketing directo.

Además, el proyecto de ley establece diferentes derechos de los titulares de los datos, obligaciones de los responsables del tratamiento de los mismos y sanciones por su incumplimiento, que en conjunto configuran la defensa de los intereses de los titulares en contra de las posibles prácticas abusivas en que el responsable pueda incurrir en el tratamiento de datos. Por ejemplo, el derecho de acceso le permite al titular solicitar al responsable de datos que le informe cuál o cuáles son sus intereses legítimos que sirven de fundamentos para efecto de realizar el tratamiento de sus datos. Asimismo, el derecho de oposición del titular lo faculta para impedir el tratamiento de datos realizado por el responsable en caso de ver afectados sus derechos o libertades, y el derecho de cancelación, que permite

al titular solicitar la supresión de los datos personales cuando haya revocado su consentimiento para el tratamiento y éste no tenga otro fundamento legal.

En relación a las obligaciones del responsable, el proyecto de ley regula, entre otras materias, el deber de informar o poner a disposición del titular, de manera expedita y cuando le sean requeridos, los antecedentes que acrediten la licitud del tratamiento de datos que realiza. En el tratamiento de datos es relevante el principio de finalidad, el cual señala que la recolección debe hacerse con fines específicos, explícitos y lícitos, limitándose a esos fines.

Otro aspecto a destacar es el sistema de sanciones que contempla el proyecto de ley. A modo de ejemplo, el tratamiento de datos personales que no cuenten con el consentimiento del titular o no tengan una base que otorgue licitud al tratamiento, constituye una infracción grave y el efectuarlo de manera fraudulenta es considerado como gravísima, lo que se podría traducir en multas de 101 a 1.000 UTM y 1.001 a 10.000 UTM, respectivamente.

Podría resultar difícil para las empresas identificar si las circunstancias que configuran el tratamiento de datos o su interés en el mismo, están tuteladas por el derecho y dentro de la esfera de la ley. Será necesario realizar una evaluación previa para verificar el objeto de la recolección de datos y determinar las circunstancias que configuran un interés legítimo en el tratamiento de los mismos. La correcta aplicación y entendimiento de la norma permitirá un ejercicio lícito del derecho de la organización a tratar datos en su actividad empresarial, evitando los riesgos de cumplimiento normativo y las respectivas multas.

Las normas de autorregulación adquieren singular relevancia ya que el proyecto de ley establece que los responsables de datos, sean personas naturales o jurídicas, públicas o privadas, deberán implementar voluntariamente mecanismos para prevenir la comisión de las infracciones contempladas en la ley. Dichos modelos deberán contener protocolos, reglas y procedimientos que permitan a las personas que intervengan en las actividades o procesos de tratamiento de datos, programar y ejecutar sus tareas o labores de una manera que prevenga la comisión de infracciones.

Complementa la norma, el hecho que los responsables del tratamiento de datos podrán atenuar su responsabilidad si acreditan haber cumplido fehacientemente sus deberes de dirección y supervisión para la protección de los datos personales bajo su responsabilidad. Se considera que los deberes de dirección y supervisión se han cumplido fehacientemente cuando, con anterioridad a la comisión de la infracción, los responsables de datos hubieren adoptado e implementado un modelo de organización, administración y supervisión para prevenir infracciones. En otras palabras, esto significa

un incentivo para el cumplimiento de la ley por parte de los responsables del tratamiento de datos.

El modelo de prevención de infracciones a la ley de protección de datos personales deberá considerar los principios de licitud, finalidad, proporcionalidad, calidad, responsabilidad, seguridad, transparencia y responsabilidad, además de los derechos del titular al acceso, rectificación, cancelación, oposición y portabilidad (ARCOP), implementando mecanismos que permitan a cada titular de datos informarse y hacer efectivos sus derechos.

Este modelo es un elemento esencial para fijar los criterios y circunstancias que determinen el interés legítimo de las empresas, estableciendo los procedimientos que describan cómo y por qué realizaran el tratamiento de datos, el análisis de riesgos, la adopción de medidas de control y supervisión, teniendo siempre en consideración las necesidades propias de las empresas y el contexto normativo vigente.

Los modelos de prevención de infracciones deben estar integrados a las políticas de la empresa y contar con el compromiso de la alta dirección de la organización, creando una cultura de cumplimiento del tratamiento de datos. Por lo tanto, al momento de pensar en la creación de un modelo eficiente, se debe contemplar la congruencia de este instrumento con aquellos protocolos y procedimientos que rigen materias que, en su conjunto, pueden impactar el tratamiento de datos, por ejemplo, el Código de Conducta de la empresa, y que conformen una jerarquía de normas internas capaces de reducir y mitigar los riesgos de cumplimiento normativo en sus diferentes dimensiones.

En definitiva, la creación de normas de autorregulación permite demostrar la proactividad de las empresas en la generación de políticas que cumplan el marco normativo vigente, incluyendo buenas prácticas y estándares éticos, obligándose a establecer medidas que garanticen la seguridad del tratamiento de datos y ejerciendo sus propios derechos e intereses de forma legítima. La autorregulación se debe entender no solo como un complemento de la ley que regula la materia; también puede significar un nivel de protección mayor a aquel entregado por las mismas normas externas y el rol fiscalizador del Estado.

SOBRE EL AUTOR



Rodrigo Medina
Gerente Legal, Supply Chain Compliance Americas.
Abogado, Universidad de Chile.
Master en Derecho, Empresa de Aix
Marseille Université .
