Nueva Ley De Protección de Datos Personales: Regulación e impacto en el mercado de seguros

Boletín N°: 33

Ene 21, 2025 CHILE

21. NOVEDAD REGULATORIA: Ley N° 21.719.

Con fecha 12 de diciembre de 2024, se ha promulgado la Ley N° 21.719, que establece una nueva regulación para la protección y el tratamiento de datos personales en Chile.

Esta norma cumple con actualizar la legislación vigente y eleva el estándar de protección a los derechos de las personas. Con la dictación de esta norma se logra un hito regulatorio relevante pues se el estándar de protección nacional se homologa al establecido por el Reglamento General de Protección de Datos de la Unión Europea, erigido como la referencia internacional para la protección de los derechos de las personas y sus datos personales.

La nueva ley establece y regula detalladamente los derechos de los titulares de los datos personales, incluyendo los de acceso, rectificación, supresión, oposición, portabilidad y bloqueo, entre otros. En adición, la ley cumple con establecer el procedimiento y los medios para que los titulares hagan valer estas garantías ante los responsables de datos.

Respecto al ámbito de sujetos a los que esta norma aplicará, se hace referencia a:

– Quienes realicen tratamiento de datos personales en el territorio nacional; y,

– Quienes realicen tratamiento de datos a nombre de un mandatario que se encuentre en el territorio nacional.

– En los casos en que el tratamiento de datos esté destinado a ofrecer bienes o servicios a personas que se encuentren en el país.

Conforme el artículo primero transitorio de la referida Ley, las obligaciones y deberes establecidas en esta norma entrarán en vigencia el día primero del mes vigésimo cuarto posterior a la publicación de esta ley en el Diario Oficial.

1. CREACIÓN DE LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES

Sabemos que existe un íntimo ámbito de conexión entre el derecho a la protección de datos personales y la obligación de seguridad en el tratamiento de estos datos, y si quisiéramos leer esto a nivel constitucional, vamos a encontrar garantías que lo explicitan (Art. 19 n°18 de nuestra Constitución relativo a la protección de la vida

privada, por ejemplo) además de existir tratados internacionales ratificados y vigentes en Chile que contienen regulación expresa en la materia (Ej. Declaración Universal de los Derechos Humanos de las Naciones Unidas, entre otras). A su vez, tal como señala Carlo Benussi Díaz (Rev. chil. derecho tecnol. vol.9 no.1 Santiago jun. 2020) el concepto de "seguridad" tiene además múltiples dimensiones, "incluyendo seguridad nacional, seguridad ciudadana, seguridad pública y la seguridad datos personales, la seguridad humana".

A partir de la realidad anterior, y conforme la relevancia práctica de la protección de datos para la vida en sociedad, la ley 21.719 cumple con complementar lo conocido desde la Ley 19.628 relativa a la Protección de Datos de Carácter personal, creando, además, una institucionalidad especial y específica destinada a proteger los derechos que a través de estas normas se consagran.

Así, se eleva a un hito fundamental de esta norma es la creación de la Agencia de Protección de Datos Personales, institución que tendrá como objetivo fiscalizar el cumplimiento de las disposiciones de esta ley y aplicar sanciones, las que se basarán en un detallado catálogo de conductas e infracciones, que se graduaran en leves, graves y gravísimas, y que se sancionarán con multas de hasta 5.000 UTM, 10.000 UTM y 20.000 UTM, respectivamente.

III. IMPACTO EN EL MERCADO ASEGURADOR:

El mercado de seguros se funda en la comercialización de pólizas, lo que dice estrecha relación con el acceso a datos personales de los contratantes, más aún respecto de canales de venta masiva. Y el acceso a información del contratante no llega sólo a su individualización, sino que se extiende a detalles respecto de sus medios de pago y/u otros detalles si estamos frente a diversas formas de ventas unificadas entre seguros y otros productos financieros.

Pensemos en un ejemplo práctico: cuando vamos a comprar remedios a una farmacia muy habitualmente damos nuestro rut para un descuento. Pues bien, en esa compra no sólo se está registrando una conducta financiera, sino además una frecuencia de compra y el tipo específico de medicamento que se adquiere, lo que permitiría generar una hipótesis de "diagnóstico simulado o supuesto" si es que a ello sumamos que, con el rut, se puede acceder a fecha de nacimiento y edad del comprador, entre otros antecedentes. ¿Qué ocurriría si esa farmacia, con la información que dispone, comienza a proponer seguros con cobertura limitada a la necesidad específica del comprador? O, en sentido contrario: ¿Qué ocurriría si a partir de los datos capturados por una farmacia un tercero, asegurador de vida y salud, limita o cancela una determinada cobertura por suponer reticencia?

La situación anterior es sólo un ejemplo baladí pues lo cierto es que, a partir de múltiples puntos de captura de datos personales (propios o de terceros) las aseguradoras podrían acceder a información tal como historial médico, ubicación o hábitos de consumo para segmentar a los clientes de forma discriminatoria.

Por lo tanto, un primer punto de relevante preocupación para los aseguradores e intermediadores de pólizas de seguros, cualquiera sea su naturaleza, dice relación con el estándar de control y cuidado respecto de los datos que se levantan para efectivamente concretar las contrataciones. Derivado de lo anterior, en caso de seguros que se sustentan en información sensible del asegurado, como en el caso de riesgos vinculados a vida y salud, se deberán proteger, además, detalles vinculados a

fichas clínicas, declaraciones personales de salud (DPS), perfilamiento de riesgos en base a patologías basales, entre otras variables de similar relevancia.

Veamos otro caso potencialmente problemático: Sabemos que actualmente se exige para cobertura de robo en vehículos la existencia de un dispositivo GPS de monitoreo constante, equipo de provee el mismo asegurador sin costo para el asegurado.

Supongamos que el asegurador, sin informar al cliente, recopila información de conducción a través del dispositivo GPS, particularmente rutas, horario de tránsito y velocidad, y luego, sin fundamento expreso, utiliza esta información para calcular primas más altas cuando el asegurado maneja de noche o excede los límites de velocidad. Esto ciertamente podría ser una hipótesis de uso de información personal sin consentimiento explícito, generando total ausencia de transparencia en el proceso de determinación de términos y condiciones de cobertura, realidad que el asegurado no conocería y que muy posiblemente redunde en una exclusión del acceso a coberturas de seguro por sus altos costos.

Así las cosas, la clave para el desarrollo y/o ejecución material del estándar de diligencia establecido en la norma en análisis implica no sólo proteger la información a la que el asegurador o intermediario tenga o pueda tener acceso sino, además, asegurar la debida transparencia, siendo esta una obligación esencial que se debe traducir en Políticas de Privacidad y Términos y Condiciones de uso de datos que sean conocidos por todos los involucrados.

En nuestra perspectiva, el estándar de diligencia establecido en esta ley no puede entenderse realizado si no se refuerzan los mecanismos de protección digital con foco en la disminución de brechas de seguridad, lo que es especialmente relevante no sólo en hipótesis de riesgos de vida o salud, sino, además, en riesgos financieros, entre otros.

Es relevante tener presente que estos deberes se extienden a todos quienes realicen tratamiento de datos personales en el territorio nacional, es decir, incluyen sin distinción a todos los actores del mercado asegurador, tanto aseguradores, como canales de venta masiva, retail, banca y, ciertamente, corredores de seguros y toda forma de intermediador de contratos asociados a la cobertura y/o transferencia de riesgos.

Así las cosas, la Ley N° 21.719 ciertamente plantea cambios relevantes los estándares actualmente conocidos de control y custodia de la información de los asegurados, lo que además se extrapola a la protección de datos de los dependientes de las compañías de seguros y demás actores del mercado, lo que supone una revolución a partir de la incorporación de roles, mecanismos de control y supervisión, prácticas y estándares que representarán un gran desafío para la industria.

Fuente

Fuente: Colegio de Corredores

Enlace:
https://colegiodecorredores.cl/nueva-ley-de-proteccion-de-datos-personales-regulacion-e-impacto-en-el-mercado-de-seguros/