Viernes 18 de mayo de 2018

Se aprobó en general el proyecto de ley que modifica la Ley de Protección de Datos: éste es su contenido

Por **GUILLERMO CAREY & PAULINA SILVA**
CAREY
Chile

En el Senado actualmente se tramita un proyecto de ley que modifica sustancialmente la Ley de Protección de Datos N° 19,628.

La Comisión de Constitución del Senado refundió en un solo texto dos proyectos de ley de modificación a la Ley de Protección de datos: la Moción de los Senadores Harboe, Araya, De Urresti, Espina y Larraín, con el Mensaje de la ex Presidenta, cuyo contenido comentamos profundamente hace un año.

El martes 3 de abril el Senado aprobó en general el texto del proyecto refundido, por 42 votos a favor y una abstención. Para que se transforme en ley falta aún la discusión en particular en el Senado, y su discusión en la Cámara de Diputados.

El siguiente es un resumen de los aspectos principales de la actual versión del proyecto de ley.

1.- Novedades del Proyecto

- Establece expresamente **principios** que regulan e informan el uso de los datos personales y **nuevos derechos** de los titulares de los datos.
- **Modifica el alcance de dato personal**: "cualquier información vinculada o referida a una persona natural, identificada o identificable", calificando esa identificabilidad cuando la identidad de la persona pueda determinarse mediante información combinada con otros datos, en particular mediante un identificador; excluyendo aquellos casos en que el esfuerzo de identificación sea desproporcionado.
- Regula en mayor detalle los **requisitos del consentimiento**, definiéndolo como una manifestación de voluntad libre, específica, inequívoca e informada; y eliminando el requisito de consentimiento escrito.
- Establece **nuevas fuentes de licitud** para el tratamiento, distintas del tratamiento binario "autorización legal o consentimiento" de la ley actual. Es decir, se establecen escenarios donde el tratamiento es autorizado aun sin requerir el consentimiento del titular.
- **Diferencia conceptualmente la cesión de la comunicación** (o transmisión) de datos personales. La cesión es el traspaso de responsable a responsable y exige el cumplimiento de requisitos especiales. La comunicación, en cambio, involucra el dar a conocer los datos "sin llegar a cederlos".
- Establece **categorías especiales de datos personales** sujetos a regulación especial: Los de niños y adolescentes; los que se utilizan con fines históricos, estadísticos o científicos; y datos de geolocalización.

- Establece y regula en forma clara los derechos de los titulares de datos: Acceso, rectificación, cancelación, oposición y portabilidad.
- Establece un nuevo derecho de **oposición a valoraciones personales automatizadas** del titular de datos a oponerse a que el responsable adopte decisiones que le afecten significativamente en forma negativa o le produzcan efectos jurídicos adversos, basadas únicamente en el tratamiento automatizado de sus datos personales, incluida la elaboración de perfiles.
- **Crea una Agencia de Protección de Datos Personales** con la capacidad de fiscalizar y sancionar los incumplimientos de la ley mediante la aplicación de multas de hasta 5.000 UTM (CLP 236.500.000, a abril de 2018).
- Crea un **Registro Nacional de Cumplimiento y Sanciones**.
- Establece **nuevos procedimientos** para perseguir responsabilidades.
- Regula por primera vez la **transferencia internacional de datos personales**.
- Establece por primera vez **deberes asociados a la seguridad de los datos**: El deber de adoptar medidas de seguridad, y obligaciones de reporte de violación de medidas de seguridad.
- Establece la posibilidad de adopción de **modelos de prevención de infracciones**, asociado a atenuantes de responsabilidad, los que deben ser certificados por la autoridad.

2.- Alcance

El proyecto regula el tratamiento de datos personales que efectúen personas naturales y jurídicas, públicas o privadas, que no se encuentren regidos por una ley especial.

La ley no se aplica al tratamiento que se realicen los medios de comunicación social en el ejercicio de las libertades de emitir opinión e informar, y al tratamiento que efectúan las personas naturales en relación con sus actividades personales.

3.- Principios

- **Principio de licitud: S**ólo puede hacerse tratamiento de datos personales con sujeción a la ley.
- **Principio de finalidad:** los datos se deben recolectar con fines específicos, explícitos y lícitos; y el tratamiento debe limitarse al cumplimiento de esos fines. Ciertas excepciones permiten tratar los datos con fines distintos a los informados, como la existencia de una relación contractual que lo justifique, o la proveniencia de los datos de una fuente de acceso público.
- **Principio de proporcionalidad: L**os datos que se traten deben limitarse a los necesarios en relación con los fines del tratamiento, y deben conservarse sólo por el tiempo que sea necesario para cumplir con esos fines. Un período de tiempo mayor requiere obtener una nueva autorización legal o consentimiento del titular.
- **Principio de calidad:** los datos personales deben ser exactos, completos y actuales, en relación con los fines del tratamiento.
- **Principio de responsabilidad:**quienes realicen tratamiento de datos personales serán legalmente responsables de cumplir con los principios y obligaciones legales.
- **Principio de seguridad:** se deben garantizar estándares adecuados de seguridad, protegiendo los datos contra el tratamiento no autorizado, pérdida, filtración, daño o destrucción, aplicando medidas técnicas u organizativas apropiadas.

- **Principio de transparencia e información:** Las políticas de tratamiento de datos deben estar permanentemente accesibles, de manera precisa, clara, inequívoca y gratuita.
- **Principio de confidencialidad:** El responsable y quienes tengan acceso a los datos deben guardar secreto acerca de aquellos. El responsable debe establecer controles adecuados para preservar el secreto. Este deber subsiste aún después de concluida la relación con el titular.

4.- Derechos de los Titulares, los "Derechos ARCOP"

Derechos personales, intransferibles e irrenunciables, pero transmisibles: Pueden ser ejercidos por los herederos del titular.

- **Derecho de acceso:** Solicitar y obtener confirmación acerca de si sus datos personales están siendo tratados, accediendo a: (i) los datos tratados y su origen; (ii) la finalidad del tratamiento; (iii) los destinatarios a quienes se han comunicado o cedido o se prevé comunicar o ceder y (iv) el periodo de tiempo durante el cual serán tratados. El proyecto contempla ciertas excepciones a este derecho.
- **Derecho de rectificación:** Derecho a solicitarla cuando los datos son inexactos, desactualizados o incompletos.
- **Derecho de cancelación:** Derecho a pedir la destrucción de los datos, en escenarios tales como (i) cuando no son necesarios en relación con los fines para el cual fueron recogidos; (ii) cuando se haya revocado el consentimiento; (iii) cuando hayan sido obtenidos o tratadas ilícitamente por el responsable; entre otros.
- **Derecho de oposición:** Derecho solicitar que no se lleve a cabo un tratamiento determinado, si (i) afecta sus derechos y libertades fundamentales; (ii) se realiza exclusivamente con fines de marketing directo, salvo que exista un contrato entre titular y el responsable; (iii) el titular de datos ha fallecido; o (iv) se realiza respecto de datos obtenidos de una fuente de acceso público.
- **Derecho de portabilidad:** Derecho a obtener una copia de los datos personales de manera estructurada, en un formato genérico y de uso común, que permita ser operado por distintos sistemas y comunicarlos a otro responsable, cuando (i) el titular haya entregado sus datos directamente al responsable; (ii) sea un volumen relevante de datos, tratados de forma automatizada; y (iii) la base el titular haya dado su consentimiento para el tratamiento o se requiera para la ejecución o el cumplimiento de un contrato.

Plazo para pronunciarse: El responsable debe pronunciarse en quince días hábiles desde la fecha de ingreso de la solicitud.

5.- Consentimiento y otras fuentes de licitud

El consentimiento es tratado como la regla general: El tratamiento es lícito si el titular otorga su consentimiento.

El consentimiento debe ser **libre, informado, específico** en cuanto a su finalidad e **inequívoco**. Con esto, se elimina el anacrónico requisito del consentimiento puramente escrito.

El consentimiento es **revocable** sin expresión de causa, pero sin efectos retroactivos.

No podrá ser el consentimiento fuente de licitud si existe un **desequilibrio ostensible** entre la posición del titular y el responsable. En estos casos, el responsable deberá acudir a otra fuente de licitud para justificar su tratamiento.

- **Otras fuentes de licitud.** Es lícito el tratamiento de datos personales, aún sin consentimiento:
  - Si los datos han sido recolectados de una **fuente de acceso público** y su tratamiento está relacionado con los fines para los cuales fueron entregados;
  - Cuando el dato es relativo a **obligaciones de carácter económico, financiero, bancario o comercial**;
  - Si el tratamiento es necesario para la ejecución o cumplimiento de una **obligación legal**;
  - Si el tratamiento es necesario para la **celebración o ejecución de un contrato** entre el titular y el responsable.
  - Si el tratamiento es necesario para la satisfacción de **intereses legítimos** del responsable o de un tercero, siempre que no se afecten los derechos y libertades del titular.
  - Si es necesario para la **defensa de un derecho en juicio**.

6.- Cesión de Datos

El proyecto no define la cesión, pero entendemos que existe cuando los datos se transfieran de un responsable a otro.

La cesión es permitida cuando (i) el titular consienta en ella y para el cumplimiento de los fines del tratamiento; (ii) sea necesaria para la ejecución de un contrato en que es parte el titular; (iii) exista un interés legítimo del cedente o del cesionario y (iv) lo disponga la ley.

La cesión debe constar por escrito o a través de cualquier medio electrónico idóneo, y debe cumplir ciertos requisitos y menciones. El cesionario adquiere la calidad de responsable respecto de los datos cedidos, y su tratamiento debe ceñirse a las finalidades del contrato cesión. El cedente mantiene la calidad de responsable respecto de las operaciones que continúe realizando.

Si se verifica una cesión de datos sin el consentimiento del titular, siendo éste necesario, la cesión será nula.

7.- Tratamiento por parte de un mandatario o encargado

Se puede efectuar el tratamiento a través de un mandatario, quien sólo puede hacerlo conforme a las instrucciones del responsable. Si el mandatario se extralimita en el tratamiento, se le considerará responsable de datos para todos los efectos, debiendo responder por las infracciones y solidariamente por los daños que ocasione, sin perjuicio de las responsabilidades contractuales que le correspondan frente al mandante.

El tratamiento que realice el mandatario se regirá por el contrato que celebre con el responsable, que deberá tener menciones especiales. La Agencia en su página web publicará modelos tipo de contratos.

El mandatario debe cumplir con las obligaciones de confidencialidad, seguridad de los datos y notificación de brechas, de la misma forma que el responsable.

8.- Obligaciones del Responsable de Datos

Entre las obligaciones del responsable de los datos, destacamos:

- **Deber de confidencialidad**respecto de los datos personales, salvo que provengan de acceso público o que el titular los haya hecho manifiestamente públicos. El responsable debe adoptar las medidas necesarias para que los dependientes bajo su responsabilidad cumplan el mismo deber.
- **Deber de información y transparencia**, manteniendo permanentemente a disposición del público información relativa a:
    - su política de tratamiento de datos, la fecha y versión;
    - la individualización del responsable, su representante legal y su encargado de prevención, si lo hubiera;
    - el medio tecnológico por el cual los titulares pueden notificarle sus solicitudes;
    - los tipos de datos que trata y sus características, los destinatarios a los que se prevé comunicarlos o cederlos, las finalidades de los tratamientos que realiza y los tratamientos que se basan en la satisfacción de intereses legítimos;
    - las políticas y las medidas de seguridad para proteger los datos que administra;
    - el derecho del titular para solicitar sus derechos ARCOP.
- **Deber de adoptar medidas de seguridad** necesarias, considerando el estado de la técnica, los costos de su aplicación, la naturaleza y los fines del tratamiento, la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos. Las medidas deben asegurar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos. El responsable tiene la carga de la prueba respecto de la existencia y funcionamiento de las medidas de seguridad.
- **Deber de reportar las vulneraciones a las medidas de seguridad** a la Agencia de Protección de Datos Personales, “sin dilaciones indebidas”, cuando:
    - la vulneración ocasione la destrucción, filtración, pérdida, alteración, comunicación o acceso no autorizado de los datos personales que trate.
    - exista un riesgo razonable que con ocasión de estos incidentes se genere un perjuicio para los titulares.

Si los datos objeto de la brecha son sensibles, o relativos a obligaciones económicas, financieras, bancarias o comerciales, el responsable debe comunicar la vulneración a los titulares, junto con las medidas para gestionarlos y precaver incidentes futuros.

9.- Datos Sensibles y Categorías Especiales de Datos

9.1 Datos Sensibles

El proyecto los define como aquellos que revelen el origen étnico o racial, la afiliación política, sindical o gremial, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género.

Los datos sensibles sólo pueden tratarse con el consentimiento expreso otorgado a través de una declaración escrita, verbal o por un medio tecnológico equivalente.

Otras bases de licitud diferentes del consentimiento para el tratamiento de datos sensibles:

- Si los datos sensibles han sido hechos manifiestamente públicos por el titular y su tratamiento esté relacionado con los fines para los cuales fueron publicados.
- El tratamiento basado en interés legítimo, realizado por una persona jurídica sin fines de lucro, bajo ciertas condiciones.
- Si el tratamiento es indispensable para resguardar la vida, salud o integridad del titular o de otra persona o el titular se encuentra física o jurídicamente impedido de otorgar su consentimiento.
- Si el tratamiento es necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia.
- Si el tratamiento es necesario para el ejercicio de derechos y el cumplimiento de obligaciones del responsable o del titular de datos, en el ámbito laboral o de seguridad social.
- Autorización legal expresa.

Otros datos sensibles con regulación especial:

- **Los datos sensibles relativos a la salud** sólo pueden ser tratados cuando sean necesarios para el diagnóstico o tratamiento médico; exista una urgencia médica; se deba calificar el grado de dependencia o discapacidad de una persona; el tratamiento sea indispensable para el cumplimiento de un contrato que exija tratar este tipo de datos; para fines históricos, estadísticos o científicos (en ciertas circunstancias); para el ejercicio o defensa de un derecho en tribunales; o cuando la finalidad del tratamiento quede establecida en la ley.
- **Los datos relativos al perfil biológico humano**, como los datos genéticos, proteómicos o metabólicos solo pueden ser tratados para realizar diagnósticos médicos, prestar asistencia en caso de urgencia, efectuar estudios o investigaciones científicas, médicas o epidemiológicas que vayan en beneficio de la salud humana o investigaciones antropológicas, arqueológicas o de medicina forense, o ejercer un derecho en tribunales.
- Quien trate **datos personales biométricos** como la huella digital, el iris, los rasgos de la mano o faciales y la voz; deberá proporcionar al titular información sobre el sistema biométrico usado, la finalidad específica de recolección, el período por el que los datos serán utilizados, y deberá cumplir con un reglamento que regulará la implementación de los sistemas biométricos.

9.2 Datos Especiales

- **Datos personales relativos a niños y adolescentes**. Por regla general, los datos de niños (hombres y mujeres menores de 14 años) sólo pueden tratarse atendiendo a su interés superior y respetando su autonomía progresiva, previa autorización de sus padres o representantes. Los datos de adolescentes (hombres y mujeres mayores de 14 y menores de 18 años) tendrán el tratamiento de los de los adultos, a excepción de sus

datos sensibles, los que deberán ser objeto de autorización de sus padres o representantes.

- **Datos tratados con fines históricos, estadísticos, científicos y de estudios o investigaciones con fines de interés público.** Existe un interés legítimo –como fuente de licitud del tratamiento distinta del consentimiento– para este tipo de tratamiento.
- Los responsables deberán adoptar y acreditar que han cumplido con todas las medidas de calidad y seguridad necesarias para resguardar que los datos se utilicen exclusivamente para tales fines, adoptando las medidas de calidad y seguridad necesarias para resguardar que se utilicen solo para esos fines; en cuyo caso el responsable podrá tratar los datos por un período indeterminado de tiempo.
- **Datos de geolocalización.** Siguen las reglas generales de bases de licitud de todo tratamiento de datos. Debe además informarse claramente al titular del tipo de datos de geolocalización que serán tratados y de la duración del tratamiento, entre otras materias.

10.- Tratamiento por Organismos Públicos

Es lícito el tratamiento de los datos personales que efectúan los órganos públicos cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias, en cuyo caso no requieren de consentimiento.

Además de los principios generales del tratamiento de datos personales, el Proyecto señala como principios orientadores del tratamiento de datos por organismos públicos los de **coordinación, eficiencia, transparencia y publicidad**.

El titular de datos podrá ejercer ante los organismos públicos los derechos de acceso, rectificación, oposición y cancelación. Estas solicitudes no serán acogidas si con ello se impide o entorpece el cumplimiento de las funciones fiscalizadoras, investigativas o sancionatorias del organismo público, o si se afecta un deber legal de secreto o reserva.

El titular podrá reclamar ante la Agencia de Protección de Datos Personales cuando el organismo público le haya denegado, en forma expresa o tácita, una solicitud en que ejerza cualquiera de los derechos que le reconoce esta ley.

El Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el Banco Central, el Servicio Electoral y la Justicia Electoral, y los demás tribunales especiales creados por ley quedan excluidos de la regulación, fiscalización o supervigilancia de la Agencia de Protección de Datos Personales.

11.- Agencia de Protección de Datos Personales

Se crea una Agencia de Protección de Datos Personales, un organismo público, autónomo, descentralizado, de carácter técnico, con personalidad jurídica y patrimonio propio, sometido a la supervigilancia del Presidente de la República a través del Ministerio de Hacienda y encargado de velar por el cumplimiento de la normativa relativa al tratamiento de datos personales y su protección. La Agencia estará afecta al Sistema de Alta Dirección Pública.

Con domicilio en Santiago, su dirección y administración superior estarán a cargo de un Director, que será el jefe superior del servicio, y que será designado por el Presidente de la República, con acuerdo del Senado, adoptado por la mayoría absoluta de sus miembros en ejercicio.

La Agencia será un órgano con amplias facultades, incluyendo:

- Aplicar e interpretar administrativamente las disposiciones legales y reglamentarias cuyo cumplimiento le corresponda vigilar.
- Impartir instrucciones generales.
- Fiscalizar el cumplimiento de los principios, derechos y obligaciones de la ley.
- Resolver las solicitudes y reclamaciones de los titulares de datos.
- Investigar y determinar las infracciones de los responsables de datos y ejercer la potestad sancionatoria de acuerdo a la ley.
- Adoptar las medidas preventivas o correctivas que disponga la ley.
- Proponer al Presidente normas legales y reglamentarias para asegurar la protección de los datos personales y perfeccionar la regulación.
- Desarrollar programas de difusión y educación en relación al respeto y protección del derecho a la vida privada.
- Administrar el Registro Nacional de Cumplimiento y Sanciones.

Se crea un **Registro Nacional de Cumplimiento y Sanciones**, de carácter público y administrado por la Agencia, que consignará las sanciones impuestas a los responsables de datos, los modelos de prevención de infracciones y los programas de cumplimiento debidamente certificados. Este registro se llevará y consultará en forma electrónica y su acceso será gratuito.

12.- Transferencia Internacional de Datos

El Proyecto regula por primera vez la transferencia internacional de datos personales, estableciendo los casos en que ella se considerará lícita.

- Cuando la trasferencia se realice a una persona sujeta al ordenamiento jurídico de un país que proporcione **niveles adecuados de protección**, entendiendo por tal a aquel que cumple con estándares similares o superiores a los de la ley de protección de datos. La Agencia determinará los países con niveles adecuados de protección de datos, considerando los elementos que establece la ley.
- Cuando quede amparada por **cláusulas contractuales** u otros instrumentos jurídicos suscritos entre el responsable que efectúa la transferencia y el que la recibe, estableciendo en ellos los derechos y garantías de los titulares, las obligaciones de los responsables y los medios de control.
- Cuando el responsable que efectúa la transferencia y el que la recibe, adopten un **modelo de cumplimiento o autorregulación vinculante** y certificado de acuerdo a la legislación de cada uno de ellos.
- Cuando exista **consentimiento expreso del titular** de datos para realizar una transferencia internacional de datos específica y determinada.
- Cuando se refiera a **transferencias bancarias, financieras o bursátiles** específicas.
- Cuando se efectúe **entre sociedades o entidades que pertenezcan a un mismo grupo empresarial**, empresas relacionadas o sujetas a un mismo controlador en los términos previstos en la Ley de Mercado de Valores, siempre que todas ellas operen bajo los mismos estándares y políticas en materia de tratamiento de datos personales. En estos casos, el responsable que efectúe la transferencia asumirá la responsabilidad

por cualquier infracción a los estándares y **políticas corporativas vinculantes** en que incurra alguno de los miembros de su grupo empresarial.
- Cuando sea necesaria para la celebración o ejecución de un contrato entre titular y el responsable, o para la ejecución de medidas precontractuales adoptadas a solicitud del titular.

La Agencia fiscalizará las operaciones de transferencia internacional, pudiendo formular recomendaciones, adoptar medidas conservativas y en casos calificados, suspender temporalmente el envío de los datos.

13.- Infracciones y Sanciones

El proyecto clasifica las infracciones **de los responsables que sean personas jurídicas privadas** en leves, graves y gravísimas, y contempla penas de **multas que van desde 1 a 5000 UTM** (aproximadamente de CLP 47.300 a CLP 236.500.000, a abril de 2018).

Se establecen criterios para la determinación de la cuantía de la multa, dentro de los cuales se contemplan **circunstancias atenuantes de responsabilidad**:

- Las acciones unilaterales de reparación y los acuerdos reparatorios convenidos entre el responsable y el titular afectado.
- La colaboración del infractor en la investigación administrativa.
- La ausencia de sanciones previas.
- La autodenuncia ante la Agencia, debiendo comunicar las medidas adoptadas para el cese de la infracción.
- El haber cumplido diligentemente sus deberes de dirección y supervisión para la protección de datos personales sujetos a tratamiento, lo que se verificará con la certificación de la Agencia para los modelos de prevención y programas de cumplimiento que reúnen los requisitos legales.

El Proyecto también establece **circunstancias agravantes de responsabilidad**:

- La reincidencia: Cuando el responsable ha sido sancionado en dos o más ocasiones en los últimos treinta meses.
- El carácter continuado de la infracción.
- El haber puesto en riesgo la seguridad de los titulares de datos personales.

Sanción de suspensión de las actividades de tratamiento de datos. Si se imponen multas por infracciones gravísimas reiteradas en un período de 24 meses, la Agencia podrá disponer la suspensión de las operaciones de tratamiento de datos que realiza el responsable hasta por 30 días, prorrogables indefinidamente por períodos de 30 días si el responsable no cumple lo dispuesto en la resolución de suspensión.

Prescripción de las acciones para sancionar las infracciones: Tres años desde la ocurrencia del hecho.

Acción por daños. Como regla general, el responsable de datos debe indemnizar el daño patrimonial y extrapatrimonial que cause al titular por infracción de la ley. Esta acción se

tramita en conformidad al procedimiento sumario, y se interpone sólo una vez ejecutoriada la resolución que resolvió favorablemente el reclamo interpuesto ante la Agencia. Las acciones civiles prescriben en tres años desde que se encuentre ejecutoriada la resolución administrativa o la sentencia judicial, según sea el caso.

14.- Nuevos Procedimientos

- **Procedimiento administrativo de tutela de derechos:** Se ejerce por el titular ante la Agencia, y procede cuando el responsable haya denegado al titular una solicitud para ejercer cualquiera de los derechos que le reconoce la ley.
- **Procedimiento administrativo por infracción de ley:** Es instruido por la Agencia como resultado de un proceso de fiscalización o a consecuencia de una reclamación presentada por un titular, para la determinación de infracciones por incumplimiento de los principios, derechos y obligaciones establecidas en la ley.
- **Procedimiento de reclamación judicial:** Las personas agraviadas por una resolución de la Agencia podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones competente, en 15 días desde la notificación de la resolución impugnada.

15.- Modelo de Prevención de Infracciones

El proyecto establece la obligación de que los responsables de datos (públicos y privados) adopten mecanismos para prevenir la comisión de infracciones; y la posibilidad de adoptar un modelo de prevención de infracciones, que deben contener elementos como la designación de un encargado de prevención; y el establecimiento de un programa de cumplimiento que identifique ciertos elementos como los tipos de datos tratados, protocolos de operación y mecanismos de reporte.

La Agencia deberá certificar que el modelo de prevención de infracciones y el programa de cumplimiento reúnen los requisitos establecidos en la ley y su reglamento, y deberá supervisar su cumplimiento.

Los responsables 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 y se considerará que esto ha sucedido si hubieren adoptado e implementado un modelo prevención de infracciones, certificado por la Agencia de Protección de Datos Personales. Estos certificados tendrán una vigencia de tres años, y bajo ciertas circunstancias podrán quedar sin efecto.

El proyecto ordena la dictación de un reglamento que establezca los requisitos, modalidades y procedimientos para la implementación, certificación, registro y supervisión de los modelos de prevención de infracciones y los programas de cumplimiento.

16.- Vigencia y artículos transitorios

El proyecto de ley entrará en vigencia en **un año** desde la publicación en el Diario Oficial.

Las bases de datos constituidas antes de la entrada en vigencia de la ley deberán adecuarse en **dos años**; sin perjuicio de que los titulares de datos puedan ejercer sus derechos ante el responsable de datos, desde la entrada en vigencia de la ley.