Consejo Federal
para la Transparencia

Informe sobre la actualización de la

Ley de Protección de Datos Personales desde una perspectiva federal

Año 2022

AAIP
Transpa rencia
Acceso a la Información Pública
Protección de Datos Personales

Argentina
Presidencia

Informe sobre la actualización de la

Ley de Protección de Datos Personales

desde una perspectiva federal

Año 2022

Autoría:

Consejo Federal para la Transparencia.

Colaboración:

Coordinador de la Comisión de Trabajo “Gobernanza de datos y protección de la privacidad”: Núñez Álvaro.

Representantes del CFT y de la Comisión “Gobernanza de datos y protección de la privacidad”: Argañaraz Romina, Briongos Marina, Martínez Miguel Ángel, Piccoli Jorge, Price María Soledad, Rezzoagli Bruno Ariel, Sepúlveda Sergio, Vázquez Ángel, Zelko Carolina.

Integrantes de la AAIP: Castro Gonzalo, Debandi Natalia, Dozo Anastasia, Dunayevich Julián, Iuliano Sara, Rosa Solange.

Diseño y arte de tapa:

Farías Vanina.

¿Cómo citar este material?

Consejo Federal para la Transparencia (2022), Informe sobre la actualización de la Ley de Protección de Datos Personales desde una perspectiva federal. Buenos Aires: Agencia de Acceso a la Información Pública.

Autoridades
del Consejo Federal para la Transparencia:

Beatriz de Anchorena
Presidenta

María Lucrecia Escandón
Vicepresidenta

Analía Zimmermann Sánchez
Secretaria Ejecutiva

Índice

1.
Introducción

Presidido por la Agencia de Acceso a la Información Pública mediante la Ley 27.275 y constituido por las 24 jurisdicciones de nuestro país, el Consejo Federal para la Transparencia es el organismo interjurisdiccional de carácter permanente que tiene como propósito la cooperación técnica y la concertación de políticas en materia de transparencia, acceso a la información pública y la protección de datos personales.

Es nuestro objetivo fortalecer las políticas de transparencia a nivel federal, a partir de un enfoque integral, que incluya no solamente el aspecto normativo, sino también la construcción de capacidades estatales para hacer efectivo el acceso a derechos a fin de lograr una mejor calidad de vida de la ciudadanía.

En la IX Asamblea, celebrada en el mes de junio, se aprobó el Plan de Trabajo para este año. En este sentido, se conformaron tres comisiones de trabajo para abordar las diferentes temáticas propias del Consejo: Transparencia, a cargo de la provincia de Salta; Gobernanza de datos y protección de privacidad, a cargo de la provincia de Jujuy; y Formación, Comunicación y Participación Ciudadana, a cargo de la provincia de Santiago del Estero.

En este marco y, a partir del inicio del proceso de debate abierto, participativo y transparente para la actualización de la Ley de Protección de Datos Personales, se seleccionaron una serie de artículos del anteproyecto de la Agencia, agrupándolos por ejes temáticos, con la finalidad de que las jurisdicciones del Consejo puedan brindar aportes y comentarios.

La nueva Ley de Protección de Datos Personales busca dar respuesta a los nuevos desafíos que imponen las transformaciones tecnológicas y el desarrollo de la economía digital y, a su vez, armonizar con estándares regionales e internacionales, desde un enfoque de derechos humanos, con una mirada situada y soberana, afianzando un camino hacia una Argentina más federal.

2.
Artículos seleccionados y comentados

2.1. Datos sensibles

ARTÍCULO 2°. - Definiciones. Datos personales sensibles: aquellos que se refieren a la esfera íntima de su Titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical u opiniones políticas; datos relativos a la salud, discapacidad, a la preferencia u orientación sexual, datos genéticos o biométricos cuando puedan revelar datos adicionales cuyo uso pueda resultar potencialmente discriminatorio para su Titular y que estén dirigidos a identificar de manera unívoca a una persona humana.

ARTÍCULO 17. - Tratamiento de datos sensibles. En el tratamiento de datos sensibles se debe implementar la responsabilidad reforzada que implica, entre otras características, mayores niveles de seguridad, confidencialidad, restricciones de acceso, uso y circulación.

Se prohíbe el tratamiento de datos sensibles, excepto si:

a) el Titular de los datos ha dado su consentimiento a dicho tratamiento, salvo en los casos en que por ley no sea requerido el otorgamiento de dicha autorización;

b) fuera necesario para salvaguardar el interés vital del Titular de los datos y éste se encontrara física o legalmente incapacitado para prestar el consentimiento y sus representantes legales no pudieran realizar en tiempo oportuno;

c) es efectuado por establecimientos sanitarios públicos o privados o por profesionales vinculados a la ciencia de la salud con la finalidad de un tratamiento médico específico de acuerdo a lo establecido por la ley Nº 26.529 de Derechos del Paciente, Historia Clínica y Consentimiento Informado y sus modificatorias: se prohíbe a los operadores de planes privados de salud tratar datos de salud para la práctica de selección de riesgo en la contratación de cualquier modalidad y la exclusión de beneficiarios;

d) Se realiza en el marco de las actividades legítimas de una fundación, asociación o cualquier otro organismo sin fines de lucro, cuyo objeto principal sea una actividad política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan un contacto regular por razón de su objeto principal, y que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los Titulares;

e) se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

f) tuviera una finalidad histórica, de archivo de interés público, estadística o científica; en estos casos y en la medida de lo posible, debe adoptarse, teniendo en cuenta la finalidad, un procedimiento de anonimización o seudonimización;

g) fuera necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del Responsable del tratamiento o del Titular de los datos en el ámbito del derecho laboral y de la seguridad, la salud pública y la protección social;

h) sea necesario en ejercicio de las funciones de los poderes del Estado en el cumplimiento estricto de sus competencias. Cuando los organismos públicos traten datos personales sensibles, deberán proveer condiciones más estrictas de seguridad, lo que debe implementarse mediante salvaguardas apropiadas adicionales, diseñadas específicamente.

i) se realiza en el marco de la asistencia humanitaria.

Comentario:

Se destaca la inclusión de los datos biométricos y genéticos en el artículo 2 que amplía la definición de datos sensibles. A su vez, se comenta sobre las características que tiene el tratamiento de estos datos de acuerdo al artículo 17°. En este sentido, se hace mención a que el tratamiento de esta categoría de datos está prohibido como principio general, excepto cuando esté determinado dentro de circunstancias específicas, entre las que el anteproyecto menciona: el consentimiento del titular de los datos, la salvaguarda del interés vital, el ejercicio de establecimientos sanitarios públicos, privados o por profesionales vinculados a la ciencia de la salud, en el marco de actividades legítimas de asociaciones y organizaciones, en un proceso judicial, cuando tenga finalidad histórica, científica, pública o estadística, para el cumplimiento de obligaciones y el ejercicio de derechos específicos del Responsable del tratamiento o del Titular, en ejercicio de las funciones de los poderes del Estado y en el marco de asistencia humanitaria. Asimismo, se destaca la incorporación del principio de "responsabilidad reforzada" para el tratamiento de datos sensibles.

2.2. Ámbito de aplicación

ARTÍCULO 3°. – Ámbito de aplicación material de la ley. La presente ley se aplica al tratamiento de datos personales, incluso si los datos personales tratados no forman parte de una base de datos o se les haya aplicado medidas de seudonimización. Se debe conciliar el derecho a la protección de datos personales con el derecho a la libertad de expresión y el acceso a la información pública. En ningún caso puede afectar el secreto de las fuentes de información periodística en el marco de esta actividad. Más allá del secreto de la fuente de información, todo otro tratamiento se encuentra alcanzado por la presente ley.

Queda exceptuado de los alcances de la presente ley el tratamiento de datos que efectúe una persona humana para su uso exclusivamente privado o de su grupo familiar y, por tanto, sin conexión alguna con una actividad profesional o comercial.

Tampoco son aplicables las disposiciones establecidas en esta ley a la información anónima ni a los datos anonimizados de forma tal que el Titular de los datos no sea identificable.

ARTÍCULO 4°. - Ámbito de aplicación territorial. La presente ley es aplicable a cualquiera de los siguientes casos:

a. Si el Responsable o Encargado del tratamiento se encuentra establecido en el territorio de la REPÚBLICA ARGENTINA, aun si el tratamiento de datos tuviese lugar fuera de dicho territorio;

b. El Responsable o Encargado, no se encuentra establecido en el territorio de la REPÚBLICA ARGENTINA, pero se da alguno de los siguientes supuestos:

I. Realiza tratamiento de datos en el territorio de la REPÚBLICA ARGENTINA mediante cualquier medio o procedimiento, físico o electrónico, conocido o por conocer, que le permite recolectar, usar, almacenar, indexar o tratar información de personas que se encuentren en dicho territorio;

II. Efectúa actividades de tratamiento relacionadas con: la oferta de bienes o servicios a personas que se encuentren en el territorio de la REPÚBLICA ARGENTINA; o el perfilamiento, seguimiento o control de los actos, comportamientos o intereses de dichas personas;

III. Se encuentra establecido en un lugar al que se aplica la legislación de la REPÚBLICA ARGENTINA en virtud del derecho internacional o de disposiciones de carácter contractual.

Comentario:

Se considera que la incorporación del concepto de "extraterritorialidad" es novedoso para el derecho internacional. Bajo este nuevo paradigma, las leyes de protección de datos personales resguardan el derecho de los titulares de derecho sin importar donde se realice el tratamiento, ni donde estén alojados sus datos. Esta inclusión se da en consonancia con los estándares internacionales y regionales en la materia y responde a las características de las actividades que se apunta a regular. En un escenario de globalización exponencial, donde el flujo de datos es el core del modelo económico global se vuelve necesario proteger el derecho de los titulares de los datos, aún cuando el tratamiento se realice fuera de las fronteras nacionales.

Lo que propone el anteproyecto es darle herramientas al Estado para regular el tratamiento de datos personales, más allá de que los responsables y los encargados estén en el territorio o no se encuentren radicados en Argentina. Esto comprende las actividades de las grandes empresas y corporaciones internacionales que en su gran mayoría no se encuentran domiciliadas en el país.

2.3. Bases legales

ARTÍCULO 13. - Bases legales para el tratamiento de datos. El tratamiento de datos personales sólo puede realizarse si se cumple al menos UNA (1) de las siguientes bases legales:

a) que el Titular de los datos otorgue su consentimiento para uno o varios fines específicos;

b) que se efectúe en ejercicio de las funciones propias de los poderes del Estado y sean necesarios para el cumplimiento estricto de sus competencias;

c) que sea necesario para el cumplimiento de una obligación legal aplicable al Responsable o Encargado del tratamiento;

d) que sea necesario para la ejecución de un contrato en el que el Titular de los datos sea parte, o para la aplicación de medidas precontractuales.

e) que resulte necesario para salvaguardar el interés vital del Titular de los datos o de terceros, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos del Titular de los datos, y este se encuentre física o jurídicamente incapacitado para otorgar su consentimiento;

f) que sea necesario para la satisfacción del interés legítimo del Responsable

del tratamiento, siempre que sobre dicho interés no prevalezcan los intereses o los derechos del Titular de los datos, en particular si el Titular es un niño, niña o adolescente. Para determinar la existencia de un interés legítimo, se debe realizar un análisis detallado, previo y documentado, que incluya el contexto y las circunstancias en las que se llevará a cabo el tratamiento, el nivel de riesgo que implica, y las expectativas razonables del Titular de los datos sobre éste, mediante la utilización de criterios de proporcionalidad y razonabilidad.

A solicitud de la Autoridad de aplicación, los Responsables tienen la carga de la prueba y deben estar en capacidad de demostrar la existencia del interés legítimo y de explicar la necesidad de recolectar o tratar los datos en cada caso.

2.4. Datos personales de niñas, niños y adolescentes

ARTÍCULO 19. - Tratamiento de datos de niñas, niños y adolescentes. En el tratamiento de datos personales de un menor o adolescente, se debe privilegiar la protección del interés superior de éstos, conforme a la CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO, aprobada por Ley Nº 23.849 y demás instrumentos internacionales de los que la Nación es parte que tiendan a garantizar su bienestar y protección integral.

1) es válido el consentimiento de menor o adolescente cuando se aplica al tratamiento de datos vinculados a la utilización de servicios de la sociedad de la información específicamente diseñados o aptos para ellos. En estos casos, el consentimiento es válido si el menor de edad tiene como mínimo TRECE (13) años. Si la niña o niño es menor de TRECE (13) años puede dar su asentimiento informado, al mismo tiempo que tal tratamiento únicamente se considera lícito si el consentimiento fue otorgado por el Titular de la responsabilidad parental o que se encuentre a cargo de su ejercicio o de la guarda o tutela sobre la niña o niño, y sólo en la medida en que se dio o autorizó.

2) el Responsable del tratamiento debe realizar esfuerzos razonables para verificar, en tales casos, que el consentimiento haya sido otorgado por el Titular de la responsabilidad parental o que se encuentre a cargo de su ejercicio o de la guarda o tutela sobre el menor o adolescente, teniendo en cuenta sus posibilidades para hacerlo.

3) se prohíbe realizar el tratamiento de datos personales de menores y adolescentes en los juegos, aplicaciones, desarrollos e innovaciones tecnológicas, u otras actividades que involucren información personal más allá de lo estrictamente necesario para el desarrollo de la actividad.

4) la información sobre el tratamiento de datos a que se refiere este artículo debe ser brindada de forma simple, clara y accesible, considerando las características físico-motoras, perceptivas, sensoriales, intelectuales y mentales del usuario, con el uso de recursos audiovisuales cuando corresponda, con el fin de brindar la información necesaria a los padres o al tutor legal o que se encuentre a cargo de su ejercicio o de la guarda o tutela y adecuado a la comprensión del menor o adolescente, de modo tal que el niño o niña pueda dar su asentimiento informado.

5) se prohíbe tratar datos sensibles de menores y adolescentes a menos que se cuente con su consentimiento o del Titular de la responsabilidad parental o que se encuentre a cargo de su ejercicio o de la guarda o tutela o cuando dicho tratamiento fuera indispensable para el interés público o para salvaguardar la vida de aquéllos o de un tercero.

6) es tarea del Estado y de las entidades educativas, proveer información y capacitar a los menores de edad y adolescentes sobre los eventuales riesgos a los que se enfrentan respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso Responsable y seguro de sus datos personales, su derecho a la privacidad, a la autodeterminación informativa y el respeto de los derechos de los demás.

Comentario:

Con el objetivo de reforzar la protección de los datos de niñas, niños y adolescentes conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales, se agrega un artículo especial relativo al tratamiento de sus datos personales. Allí se reconoce la posibilidad de brindar consentimiento a partir de los 13 años y se enfatiza sobre la obligación del responsable de informar de manera pedagógica y clara teniendo en consideración las características físico-motoras, perceptivas, sensoriales, intelectuales y mentales del usuario.

Esto último (contemplado en el inciso 1 del art. 19 del proyecto) es concordante con lo establecido en el Código Civil y Comercial, que reconoce que las personas menores de edad tienen capacidad progresiva, entendiéndose que la capacidad de ejercicio no se adquiere instantáneamente al alcanzar la mayoría de edad (cumplir 18 años), sino que se trata de un proceso gradual, por el cual las personas menores de edad pueden ir ejerciendo derechos por sí mismas conforme a su edad y grado de madurez.

Asimismo, se explicita la responsabilidad del Estado y las instituciones educativas de proveer información y capacitar a los menores de edad y adolescentes sobre los eventuales riesgos a los que se enfrentan ante el tratamiento indebido de sus datos personales.

Este artículo se nutre de los aportes de las legislaciones regionales, en particular Ecuador y Brasil, así como también de las propuestas presentadas por diferentes legisladoras y legisladores nacionales.

2.5. Notificación de incidentes de seguridad

ARTÍCULO 21. - Notificación de incidentes de seguridad. En caso de que ocurra un incidente de seguridad de datos personales, el Responsable del tratamiento debe notificarlo a la Autoridad de aplicación dentro de las SETENTA Y DOS (72) horas de haber tomado conocimiento de aquél.

En caso de no contar con los medios materiales para cumplir el plazo previsto, debe justificar a la Autoridad de aplicación la extensión de éste. Si la notificación a la Autoridad de aplicación no tiene lugar en el plazo previsto, debe ir acompañada de indicación de los motivos de la dilación. De igual manera, el Responsable del tratamiento debe informar al Titular de los datos sobre el incidente de seguridad ocurrido, en un lenguaje claro y sencillo.

Si ello supone un esfuerzo desproporcionado dicha notificación puede realizarse mediante una comunicación pública, en la medida en que la misma sea igualmente efectiva para informar al Titular de la incidencia.

La notificación debe contener, al menos, la siguiente información:

a) la naturaleza del incidente;

b) los datos personales que pueden estimarse comprometidos;

c) las acciones correctivas realizadas de forma inmediata;

d) las recomendaciones al Titular de los datos acerca de las medidas que éste puede adoptar para proteger sus intereses;

e) los medios a disposición del Titular de los datos para obtener mayor información al respecto, incluido el nombre y datos de contacto del Delegado de protección de datos o cualquier otro designado como contacto.

El Responsable del tratamiento debe documentar todo incidente de seguridad que ponga en alto riesgo los derechos de los Titulares ocurrido en cualquier fase del tratamiento de datos e identificar, de manera enunciativa pero no limitativa, la fecha en que ocurrió, el motivo del incidente, los hechos relacionados con éste y sus efectos y las medidas correctivas implementadas de forma inmediata y definitiva. En caso de que no sea posible enviar toda la información

detallada al mismo tiempo, la persona Responsable puede enviarla sin dilación alguna, a medida que sea posible.

Comentario:

Forma parte de una perspectiva de seguridad e integridad de los datos personales desde una lógica de responsabilidad proactiva. La notificación de las brechas de seguridad de los datos personales, junto con las obligaciones establecidas al titular como la designación de un delegado de protección de datos personales, la evaluación de impacto, así como los conceptos de protección de datos desde el diseño y por defecto.

Se deja atrás un enfoque regulatorio que trata a todos los responsables de tratamiento y a todas las actividades de tratamiento por igual, y pone el foco en el riesgo que las actividades de tratamiento pueden tener para los derechos de las personas.

2.6. Transferencias internacionales

ARTÍCULO 23. - Principio general de las transferencias internacionales. Las transferencias de datos personales fuera del territorio nacional, incluidas las transferencias ulteriores se pueden realizar en cualquiera de los siguientes supuestos:

a) si el país u organismo internacional o supranacional receptor proporciona un nivel de protección adecuado;

b) si exportador ofrece garantías apropiadas al tratamiento de los datos personales, en cumplimiento de las condiciones mínimas y suficientes establecidas en esta ley;

c) las excepciones para situaciones específicas determinadas en el artículo 25 de la presente ley.

A efectos de demostrar que la transferencia internacional sea realizada conforme a lo que establece ésta ley, la carga de la prueba recae, en todos los casos, en el exportador.

Quien realiza transferencias internacionales de datos debe implementar medidas para garantizar los derechos de los Titulares y responde frente a su eventual vulneración.

ARTÍCULO 24. - Transferencias internacionales basadas en una decisión de adecuación.

La Autoridad de aplicación será quien determine la condición de país adecuado, teniendo en cuenta los siguientes elementos:

a) el estado de derecho, el respeto de los derechos humanos y las libertades fundamentales;

b) la legislación vigente, tanto general como sectorial, incluidas las limitaciones y garantías para el acceso de las autoridades públicas a los datos personales;

c) la existencia de garantías judiciales e institucionales para el respeto de los derechos de protección de datos personales;

d) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el país u organización que reciba la información, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los Titulares de los datos en el ejercicio de sus derechos, y de cooperar con la Autoridad de aplicación.

ARTÍCULO 25. - Transferencias internacionales mediante garantías adecuadas. A falta de una decisión de adecuación, las garantías adecuadas pueden ser aportadas por:

a) un instrumento jurídicamente vinculante y exigible entre autoridades u organismos públicos de la REPÚBLICA ARGENTINA y otros países, que contenga los principios, derechos y obligaciones establecidos en la presente ley;

b) un acuerdo internacional bilateral o multilateral, entre la REPÚBLICA ARGENTINA y otros países u organizaciones internacionales, que contenga los principios,obligaciones y establecidos en la presente ley, y que habilite las transferencias desde entidades privadas /o públicas establecidas en Argentina hacia entidades privadas y/o públicas establecidas en otros países;

c) acuerdos o convenios que expresamente reconozcan los principios,derechos y obligaciones establecidos en la presente ley, los que pueden adoptar las siguientes formas:

I. Cláusulas contractuales modelo que hayan sido previamente aprobadas por la Autoridad de aplicación;

II. normas corporativas vinculantes que hayan sido aprobadas por la Autoridad de aplicación y que se apliquen a todos los miembros de un grupo económico en los términos que establece la presente ley;

III. mecanismos de certificación en materia de protección de datos aprobados por la Autoridad de aplicación.

En los casos de transferencias regidas por el presente artículo, el acuerdo o mecanismo que la transferencia, debe reconocer que la parte exportadora se encuentra sujeta a la jurisdicción de la Autoridad de aplicación y de los tribunales de la REPÚBLICA ARGENTINA competentes y asegurar que la parte importadora se encuentre sujeta a la jurisdicción de una o varias autoridades de supervisión independientes de manera que los Titulares de los datos cuenten con acciones legales efectivas para proteger sus derechos.

ARTÍCULO 26. - Excepciones. Las transferencias internacionales pueden realizarse excepcionalmente si se cumplen algunas de las siguientes condiciones:

a) que el Titular de los datos haya otorgado su consentimiento;

b) que la transferencia sea necesaria para la ejecución de un contrato entre el Titular de los datos y el Responsable del tratamiento, o en beneficio del Titular de los datos, entre el Responsable de tratamiento y otra persona humana o jurídica, o para la ejecución de medidas precontractuales adoptadas a solicitud del Titular de los datos;

c) que la transferencia sea necesaria:

(I) por razones de interés público;

(II) para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; o

(III) para proteger los intereses vitales del Titular de los datos o de otras personas, si estuviera física o jurídicamente incapacitado para otorgar su consentimiento.

Las condiciones establecidas en el presente artículo deben estar siempre sujetas al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad. Las excepciones enumeradas en el presente artículo no pueden ser utilizadas para realizar transferencias internacionales de forma periódica o habitual, ni si involucran a un gran número de personas.

Comentario:

El nuevo anteproyecto de ley pretende brindar claridad en relación a cuáles son los mecanismos para realizar la transferencia de datos a nivel internacional

de manera adecuada, garantizando y salvaguardando los derechos de los titulares de los datos.

Conscientes que el flujo transfronterizo es el núcleo de la economía digital se detallan tres mecanismos con distintas jerarquías a través de los artículos 24, 25 y 26.

En primer lugar, para aquellos países que presenten garantías legales, de tal forma que permitan a la Agencia determinarlos como países con garantías adecuadas, como son el respeto a los derechos humanos, autoridades independientes, legislaciones que protejan los datos personales y la privacidad de las personas.

El segundo mecanismo, aplica en aquellos caso en los que el país destinatario no cumpla los estándares de legislación adecuada, consiste en implementar mecanismos que aseguren las garantías necesarias, esto puede darse a través de cláusulas contractuales, normas corporativas vinculantes o certificaciones de que el tratamiento de determinados datos o , por ejemplo, de determinadas empresas, están certificadas y son las adecuadas. En todos los casos, será la autoridad de aplicación quien apruebe estos mecanismos.

Por último, establece un mecanismo de excepciones que tienen lugar bajo ciertas condiciones y no pueden ser utilizadas de manera periódica.

2.7. Derechos de los titulares de los datos

ARTÍCULO 27. - Derecho de acceso. El Titular de los datos, previa acreditación de su identidad, tiene el derecho de solicitar y obtener confirmación de si se están tratando o no sus datos personales, y en tal caso, el derecho de acceso a ellos, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento. Tiene derecho a obtener la siguiente información sobre el tratamiento de sus datos:

a) las finalidades del tratamiento y las bases legales que legitiman cada finalidad;

b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a los que se cedieron o se prevean ceder los datos personales;

d) la relativa a las transferencias internacionales de datos que se hayan efectuado o se prevea efectuar, con inclusión de países de destino y base legal que justifica la transferencia;

e) el plazo previsto de conservación de los datos personales o, de no ser ello posible, los criterios utilizados para determinar este plazo;

f) la existencia del derecho a solicitar del Responsable del tratamiento la rectificación, supresión de datos personales o a oponerse a dicho tratamiento;

g) el derecho a iniciar un trámite de protección de datos personales ante la Autoridad de aplicación;

h) si los datos personales no se han obtenido del Titular de los datos, cualquier información disponible sobre su origen;

i) la existencia de decisiones automatizadas, incluida la elaboración de perfiles a que se refiere el artículo 31 y, al menos en tales casos, información significativa sobre la lógica aplicada, sin que ello afecte derechos intelectuales del Responsable del tratamiento.

En ningún caso el informe puede revelar datos pertenecientes a terceros, aun si se vinculan con el Titular de los datos. La información, a opción del Titular de los datos, puede entregarse por escrito, por medios electrónicos, telefónicos, de imagen u otro idóneo para tal fin.

ARTÍCULO 28. - Derecho de rectificación. El Titular de los datos tiene el derecho a obtener del Responsable del tratamiento la rectificación de sus datos personales, si éstos resultan ser inexactos, falsos, errados, incompletos o no se encontrarán actualizados.

En el supuesto de cesión o transferencia internacional de datos erróneos o desactualizados, el Responsable del tratamiento debe notificar la rectificación al cesionario dentro del plazo de CINCO (5) días hábiles de haber tomado conocimiento efectivo del error o la desactualización.

Durante el proceso de verificación y rectificación de la información de que se trate, el Responsable debe bloquear el dato, o bien consignar, al proveer información relativa a éste, la circunstancia de que se encuentra sometido a revisión.

ARTÍCULO 29. - Derecho de oposición. El Titular puede oponerse al tratamiento de sus datos o de una finalidad específica de éste, si no ha prestado consentimiento. El Responsable del tratamiento debe dejar de tratar los datos personales objeto de oposición, salvo que existan motivos legítimos para el tratamiento que prevalezcan sobre los derechos del Titular de los datos.

El Titular también puede oponerse al tratamiento de sus datos personales si tuvieran por objeto la publicidad, la prospección comercial o la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada

con esas finalidades. Cuando el Titular se oponga al tratamiento para esos propósitos, sus datos personales deben dejar de ser tratados para dichos fines.

El Titular tiene derecho a que el tratamiento de datos personales se limite a su almacenamiento durante el período que medie entre una solicitud de rectificación u oposición hasta su resolución por el Responsable.

ARTÍCULO 30. - Derecho de supresión. El Titular de los datos tiene derecho a solicitar la supresión de sus datos personales al Responsable del tratamiento.

La supresión procede sí:

a) los datos personales ya no son necesarios en relación con los fines para los que fueron recolectados;

b) el Titular de los datos revoca el consentimiento en que se basa el tratamiento de datos y éste no se ampara en otra base legal;

c) el Titular de los datos ha ejercido su derecho de oposición conforme al artículo 29, y no prevalecen otros motivos legítimos para el tratamiento de sus datos;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal o por orden de autoridad competente;

f) los datos son tratados para fines de publicidad, prospección comercial o mercadotecnia.

La supresión no procede si pudiese causar perjuicios a derechos o intereses legítimos de terceros, si prevalecen razones de interés público para el tratamiento de datos cuestionado, o si los datos personales deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las contractuales entre el Responsable o Encargado del tratamiento y el Titular de los datos, o si son necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística, siempre que no pueda aplicarse el proceso de anonimización o seudonimización.

La supresión tampoco procede si el dato es necesario para el esclarecimiento de violaciones de derechos humanos, genocidio, crímenes de guerra o delitos de lesa humanidad.

ARTÍCULO 31. - Decisiones automatizadas y elaboración de perfiles. El Titular de los datos tiene derecho a no ser objeto de una decisión basada única o parcialmente en el tratamiento automatizado de datos, incluida la elabora-

ción de perfiles e inferencias, que le produzca efectos jurídicos perniciosos, lo afecte significativamente de forma negativa o tengan efectos discriminatorios. Se entiende por decisiones parcialmente automatizadas o semiautomatizadas aquellas en las que no hay intervención humana significativa.

El interesado tiene derecho a solicitar la revisión por una persona humana de las decisiones tomadas sobre la base del tratamiento automatizado o semiautomatizado que afecten a sus intereses, incluidas las decisiones encaminadas a definir sus aspectos personales, profesionales, de consumo, de crédito, de su personalidad u otros.

El Responsable del tratamiento debe proporcionar, siempre que se le solicite, información clara, completa y adecuada sobre los criterios y procedimientos utilizados para la decisión automatizada o semiautomatizada, con observancia de secretos comerciales e industriales.

En caso de no proporcionar la información a que se refiere este artículo con base en la observancia del secreto comercial e industrial, la Autoridad de aplicación puede realizar auditorías para verificar, entre otros, aspectos discriminatorios o de contenido erróneo o sesgado, en el tratamiento automatizado o semiautomatizado de información personal.

El Responsable del tratamiento debe adoptar las medidas adecuadas para salvaguardar los derechos del Titular de los datos; como mínimo, el derecho a obtener intervención humana por parte del Responsable del tratamiento, a expresar su punto de vista y a impugnar la decisión.

El Responsable del tratamiento no puede llevar a cabo tratamientos automatizados o semiautomatizados de datos personales que tengan como efecto la discriminación en detrimento de los Titulares de los datos, particularmente si se encuentran basados en alguna de las categorías de datos contenidas en la definición de datos sensibles del artículo 2 de la presente ley.

ARTÍCULO 32. - Derecho a la portabilidad de datos personales. Si se tratan datos personales mediante medios electrónicos o automatizados, el Titular de los datos tiene derecho a obtener una copia de los datos personales que hubiere proporcionado al Responsable o que sean objeto de tratamiento, en un formato que le permita su ulterior utilización por parte de otro Responsable.

El Titular de los datos puede solicitar que sus datos personales se transfieran directamente de Responsable a Responsable si ello fuera técnicamente posible.

Este derecho no procede sí:

a) su ejercicio impone una carga financiera o técnica excesiva o irrazonable sobre el Responsable o Encargado del tratamiento;

b) vulnera la privacidad de otro Titular de los datos;

c) afecta las obligaciones legales del Responsable del tratamiento; d. Impide que el Responsable del tratamiento proteja sus derechos, seguridad, bienes, o los del Encargado del tratamiento, o del Titular de los datos o de un tercero. Sin perjuicio de otros derechos del Titular, el derecho a la portabilidad de los datos personales no es procedente si se trata de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el Responsable con base en los datos personales del Titular.

ARTÍCULO 33. - Derecho de limitación. El interesado tiene derecho a obtener del Responsable la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) si el Titular impugna la exactitud de los datos personales, durante un plazo que permita al Responsable verificar la exactitud de los mismos;

b) si el tratamiento es ilícito y el interesado se opone a la supresión de los datos personales y solicita en su lugar la limitación de su uso;

c) si el Responsable ya no necesita los datos personales para los fines del tratamiento, pero el interesado los necesita para la formulación, el ejercicio o la defensa de sus derechos;

d) si el interesado se ha opuesto al tratamiento en virtud del artículo 29, mientras se verifica si los motivos legítimos del Responsable prevalecen sobre los del interesado. Todo interesado que haya obtenido la limitación del tratamiento debe ser informado por el Responsable antes del levantamiento de dicha limitación.

En caso que el Titular recurra ante la Autoridad de aplicación por la negativa del Responsable o Encargado del tratamiento, esta limitación se extenderá hasta la resolución del procedimiento administrativo.

Comentario:

El nuevo Anteproyecto amplía y desarrolla los derechos ARCO (Acceso, Rectificación, Cancelación/supresión y Oposición) presentes en la vigente ley de Protección de Datos Personales e incorpora el derecho a la portabilidad y de limitación.

Además, se establece el derecho a oponerse a ser objeto de una decisión basada única o parcialmente en el tratamiento automatizado de datos, incluida la elaboración de perfiles e inferencias, así como también a solicitar la inter-

vención humana para la revisión de estas decisiones. A su vez, el anteproyecto obliga al responsable a brindar información clara, completa y adecuada sobre los criterios y procedimientos utilizados cuando el titular de los datos tratados se lo solicite.

En cuanto a los criterios de aplicación del derecho a la supresión en la gestión pública, se destaca la necesidad de documentar los procesos y tener en cuenta las implicancias en términos tecnológicos.

El derecho a la supresión procede ante ciertas condiciones, es decir, la supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, prevalezcan razones de interés público para el tratamiento de datos cuestionado, o los datos personales deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las contractuales entre el Responsable o Encargado del tratamiento y el Titular de los datos, o cuando sean necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística, siempre que no pudiera aplicarse el proceso de anonimización.

Al mismo tiempo, la supresión tampoco procede en temas vinculados a memoria, verdad y justicia y de los Derechos Humanos en general.

Asimismo se destaca la diferencia entre la confidencialidad de los datos y la supresión, es decir, la eliminación de un dato de una base de datos.

2.8. Obligaciones de los responsables y encargados del tratamiento

ARTÍCULO 36. - Deberes del Responsable del tratamiento. Los Responsables del tratamiento deben cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley, sus normas reglamentarias y otras que rijan su actividad:

a) implementar medidas apropiadas, útiles, oportunas, pertinentes y eficaces para garantizar y poder demostrar el adecuado cumplimiento de la presente ley y sus normas reglamentarias, especialmente los derechos de los Titulares y la materialización de los principios del tratamiento de datos personales;

b) garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de protección de datos, especialmente conocer, actualizar, rectificar, suprimir sus datos personales u oponerse al tratamiento de éstos;

c) cumplir con el deber de informar al Titular sobre la finalidad de la recolección y sus derechos;

d) tratar los datos personales bajo condiciones de seguridad apropiadas necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

e) implementar medidas para garantizar que los datos personales sean veraces, actualizados, completos, exactos y comprobables;

f) actualizar los datos personales, rectificar la información si fuera incorrecta y adoptar medidas necesarias para que ésta se mantenga actualizada;

g) tramitar debidamente las solicitudes presentadas por el Titular, y responderlas de manera completa y oportuna;

h. Notificar en plazo de ley a la Autoridad de aplicación y a los Titulares los incidentes de seguridad ocurridos, de acuerdo al artículo 21;

i) cumplir las instrucciones, órdenes o requerimientos que imparta la Autoridad de aplicación.

j) formalizar mediante la suscripción de un acuerdo, contrato o cualquier otro instrumento jurídico la prestación de servicios entre el Responsable y el Encargado.

k) verificar que los Encargados, o quienes éstos subcontraten, ofrezcan garantías suficientes para realizar el tratamiento de datos personales conforme a los requisitos de la presente ley y garanticen la protección de los derechos del Titular; dicha verificación debe realizarse con anterioridad a la contratación o realización de otro acto jurídico que lo vincule con el Encargado;

l) exigir al Encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y debido tratamiento de la información del Titular;

m) en caso de que corresponda, designar un Delegado de Protección de Datos.

En caso de no corresponder, se debe establecer una persona o área que asuma la función de protección de datos personales, y de trámite a las solicitudes de los Titulares. Si el tratamiento de datos consiste en una cesión, el Responsable del tratamiento a quien se ceden los datos personales queda sujeto a las mismas obligaciones legales y reglamentarias que el cedente. Ambos responden por la observancia de aquéllas ante la Autoridad de aplicación y el Titular de los datos de que se trate. En cualquier caso, pueden ser eximidos total o parcialmente de responsabilidad si demuestran que no se les puede imputar el hecho que ha producido el daño.

ARTÍCULO 37. - Deberes del Encargado de tratamiento. Los Encargados del tratamiento deben cumplir las siguientes condiciones al realizar el tratamiento de datos personales, sin perjuicio de las demás disposiciones previstas en la presente ley, sus normas reglamentarias y otras que rijan su actividad:

a) la prestación de servicios de tratamiento de datos por cuenta de terceros entre un Responsable y un Encargado del tratamiento debe quedar formalizada mediante un contrato por escrito y no requiere del consentimiento del Titular de los datos;

b) el Encargado se encuentra limitado a llevar a cabo sólo aquellos tratamientos de datos encomendados por el Responsable del tratamiento;

c) los datos personales objeto de tratamiento no pueden aplicarse o utilizarse con un fin distinto al que figure en el contrato ni ser cedidos a otras personas, ni aun para su conservación, salvo autorización expresa del Responsable del tratamiento;

d) una vez cumplida la prestación contractual, los datos personales tratados deben ser devueltos al Responsable o destruidos, salvo que medie autorización expresa del Responsable cuando razonablemente se pueda presumir la posibilidad de ulteriores encargos, en cuyo caso sólo podrán conservarse por un máximo de DOS (2) años;

e) permitir al Responsable o Autoridad de aplicación realizar inspecciones o auditorías para verificar el cumplimiento de la ley y de lo pactado en el contrato de prestación de servicios; f) el Encargado puede suscribir un contrato para subcontratar servicios que impliquen el tratamiento de datos solamente cuando exista una autorización expresa del Responsable del tratamiento. En estos casos el subcontratado asume el carácter de Encargado en los términos y condiciones previstos en esta ley. Para el supuesto en que el subcontratado incumpla sus obligaciones y responsabilidades respecto al tratamiento de datos que lleve a cabo conforme a lo estipulado en el contrato, asume la calidad de Responsable del tratamiento en los términos y condiciones previstos en la presente ley. Los contratos previstos en este artículo deben estipular el objeto, alcance, contenido, duración, naturaleza y finalidad del tratamiento de datos, el tipo de datos personales, las categorías de los datos, el cumplimiento del deber de confidencialidad y demás obligaciones y responsabilidades del Responsable y Encargado del tratamiento;

g) implementar medidas apropiadas, útiles, oportunas, pertinentes y eficaces para garantizar y poder demostrar el adecuado cumplimiento de la presente ley y sus normas reglamentarias, especialmente los derechos de los Titulares y la materialización de los principios del tratamiento de datos personales;

h) tratar los datos personales bajo condiciones de seguridad apropiadas para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

i) cumplir las instrucciones, órdenes o requerimientos que imparta la Autoridad de aplicación;

j) tramitar debidamente las solicitudes presentadas por el Titular, notificando al Responsable del tratamiento y dando aviso al Titular de dicha notificación;

k) informar cabalmente y en plazo de ley a la Autoridad de aplicación y al Responsable del tratamiento cuando se presenten incidentes de seguridad y existan riesgos en la administración de la información de los Titulares;

l) en caso de que corresponda, designar un Delegado de Protección de Datos.

En caso de no corresponder la designación de un Delegado de Protección de Datos, se debe establecer una persona o área que asuma la función de protección de datos personales y trámite las solicitudes de los Titulares.

Comentario:

Los cambios regulatorios en materia de protección de datos personales centran su atención en las obligaciones del responsable de tratamiento y profundizan en las acciones que debe llevar a cabo para preservar la seguridad de los datos personales y el respeto a la privacidad de los titulares.

El nuevo proyecto profundiza en las obligaciones de los responsables y encargados del tratamiento. Para eso, se incorpora el concepto de responsabilidad proactiva, que obliga a la adopción de procesos internos para llevar adelante de manera efectiva las medidas de responsabilidad, así como la realización de supervisiones o auditorías, internas o externas, para controlar el cumplimiento de las medidas adoptadas. Es decir, no solo se deben implementar las medidas, sino que también el responsable tiene a su cargo la obligación de demostrar a la autoridad que lo ha realizado.

A su vez, el artículo 40 introduce la protección de datos desde el diseño y por defecto, a fin de aplicar medidas tecnológicas y organizativas apropiadas para garantizar la protección y privacidad de los datos de los interesados antes de llevar a cabo el tratamiento de dichos datos.

Esto quiere decir que al diseñar una plataforma, aplicación o medio a través del cual se tratan datos personales, se deben diseñar también las medidas de seguridad necesarias para garantizar la privacidad de los titulares de los datos.

La privacidad por defecto implica que el responsable y el encargado del tratamiento debe aplicar las medidas tecnológicas y organizativas apropiadas con miras a garantizar que, por defecto, sólo sean objeto de tratamiento de datos aquellos datos personales que sean necesarios para cada uno de los fines del tratamiento. Esta obligación se aplica a la cantidad y calidad de datos personales tratados, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.

El artículo 41 incluye la evaluación de impacto relativa a la protección de los datos y la establece como obligatoria en los siguientes casos, sin perjuicio de otros que determine la autoridad de aplicación:

a. Evaluación sistemática y exhaustiva de aspectos personales de personas humanas que se base en un tratamiento de datos automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas humanas o que les afecten significativamente de modo similar.

b. Tratamiento de datos sensibles a gran escala, o de datos relativos a antecedentes penales o contravencionales.

c. Observación sistemática a gran escala de una zona de acceso público.

El fundamento de esta medida está asociado a la idea de que cuanto mayor sea el riesgo que implica el tratamiento de esos datos, mayores deben ser las obligaciones a cargo de los responsables y/o encargados.

A su vez, el artículo 44 presenta la figura de Delegado de Protección de Datos Personales, que debe ser designado cuando:

- el tratamiento lo lleve a cabo una autoridad u organismo público,

- se realice un tratamiento de datos sensibles como parte de la actividad principal o

- se realice tratamiento de datos a gran escala.

El mismo debe ser una persona humana que reúna los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones.

La ley establece sus funciones en el artículo 43.

Finalmente, el artículo 46 exige a los responsables y encargados del tratamiento que no están establecidos en Argentina la designación de un representante en el país. El artículo en su parte pertinente dice:

“Cuando el responsable o el encargado del tratamiento no se encuentren

establecidos en la República Argentina conforme a lo normado en el artículo 4, inciso b de la presente Ley, deberá designar un representante en la REPÚBLICA ARGENTINA, quien actuará en nombre de ellos.

El presente artículo no será aplicable cuando:

a) El tratamiento sea ocasional, no incluya el manejo a gran escala de categorías de datos sensibles o personales relativos a condenas e infracciones penales, y que sea improbable que entrañe un riesgo para los derechos y libertades de las personas humanas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento.

b) Se trate de organismos públicos extranjeros."

La figura del representante sirve para notificar a las empresas extranjeras, reafirmar la aplicación de la ley en forma extraterritorial y permite que la Agencia de Acceso a la Información Pública tenga un canal directo con empresas no presentes en Argentina pero que tratan datos de argentinos o quienes residan en el país.

El Representante es una figura que aparece en el Reglamento General de Protección de Datos, art. 27 con la finalidad de que las empresas que no están físicamente en el territorio pero que operan en el mismo cumplan con la ley (por art. 3.2 del Reglamento General de Protección de Datos se les aplica por el principio de extraterritorialidad).

2.9. Delegado de protección de datos

ARTÍCULO 44. - Delegado de protección de datos. Los Responsables y Encargados del tratamiento deben designar un Delegado de protección de datos en cualquiera de los siguientes supuestos:

a. Si se trata de una autoridad u organismo público;

b. Las actividades del Responsable o Encargado del tratamiento de datos personales requieran un control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades, conforme a lo que se establezca en esta ley, su reglamentación, o en la normativa que dicte al respecto la Autoridad de aplicación.

Si los Responsables y Encargados del tratamiento no se encuentran obligados a la designación de un Delegado de protección de datos de acuerdo a lo previsto en este artículo, pueden designar de manera voluntaria o por orden expresa de la Autoridad de aplicación.

En el caso en que se trate de una autoridad u organismo público con dependencias subordinadas, se puede designar un único Delegado de protección de datos, teniendo en consideración su tamaño y estructura organizativa.

Un Grupo económico puede nombrar un único Delegado de protección de datos siempre que esté en contacto permanente con cada una de las empresas que lo componen.

La designación del Delegado de protección de datos debe recaer en una persona que reúna los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones. Las funciones del Delegado de protección de datos pueden ser desempeñadas por un empleado del Responsable o Encargado del tratamiento o en el marco de un contrato de prestación de servicios.

El Delegado de protección de datos puede ejercer otras funciones siempre que no den lugar a conflictos de intereses.

El Responsable o Encargado del tratamiento está obligado a respaldar al Delegado de protección de datos personales en el desempeño de sus funciones, y a facilitarle los recursos necesarios para su desempeño y para el mantenimiento de sus conocimientos especializados y la actualización de éstos.

El Delegado debe ejercer sus funciones de manera autónoma y libre de interferencias, sin recibir instrucciones, y sólo debe responder ante el más alto nivel jerárquico de la organización. No puede ser destituido ni sancionado por desempeñar sus funciones.

ARTÍCULO 45. - Funciones del Delegado de protección de datos. El Delegado de protección de datos tiene las siguientes funciones, sin perjuicio de otras que se le asignen especialmente:

a. Informar y asesorar a los Responsables y Encargados del tratamiento, así como a sus empleados, de las obligaciones a su cargo;

b. Promover y participar en el diseño y aplicación de una política de tratamiento de datos personales;

c. Supervisar el cumplimiento de la presente ley y de la política de protección de datos;

d. Asignar responsabilidades, concientizar, formar al personal y realizar las auditorías correspondientes;

e. Ofrecer el asesoramiento que se le solicite para hacer una evaluación de

impacto relativa a la protección de datos, cuando entrañe un alto riesgo de afectación para los derechos de los Titulares, y supervisar luego su aplicación;

f. Cooperar y actuar como referente ante la Autoridad de aplicación para cualquier consulta sobre el tratamiento de datos efectuado por el Responsable o Encargado del tratamiento.

Comentario:

Respecto de esta figura, los integrantes de la comisión manifiestan dudas en relación a los criterios de implementación del delegado de protección de datos. Se aclara que estas cuestiones forman parte de una etapa posterior al anteproyecto correspondiente a su reglamentación.

Se destaca que no resulta necesario crear un departamento específico, sino que es suficiente que una persona que ya se encuentra dentro del organismo sea designada al efecto. Además, el anteproyecto contempla la posibilidad de que el agente cumpla diferentes roles siempre y cuando no tengan incompatibilidad. Lo prioritario es que el delegado se capacite en la materia.

El proyecto prevé la designación, por parte de los Responsables y Encargados del tratamiento, de un Delegado de protección de datos en determinados supuestos. Ese delegado tiene como rol principal promover y participar en el diseño y aplicación de una política de tratamiento de datos personales; además de ejercer tareas de asesoramiento a responsables y encargados del tratamiento y de control y supervisión en lo que respecta al cumplimiento de la Ley y de la política de protección de datos.

En este sentido, pueden considerarse como antecedentes figuras análogas previstas en materia de acceso a la información y de ética pública.

En acceso a la información (Ley N° 27.275), existe el Responsable de Acceso a la Información Pública, dentro del ámbito de cada sujeto obligado, quién además de tramitar las solicitudes de acceso a la información pública dentro de su jurisdicción, realiza tareas de seguimiento y control de la correcta tramitación de las solicitudes, promover la implementación de las resoluciones elaboradas por la Agencia, etc.

En materia de ética pública, se establece la figura del Enlace de Integridad en las distintas Jurisdicciones y Entidades que conforman la Administración Pública Nacional (Decreto N° 650/2019), cuya función consiste en la implementación de estrategias de sensibilización y capacitación en temas de "transparencia, ética y lucha contra la corrupción" y la promoción del cumplimiento de las obligaciones y recomendaciones internacionales en materia de lucha contra la corrupción, en el ámbito de su competencia.

2.10. Vigencia

ARTÍCULO 74. - Vigencia. La presente ley entrará en vigencia el día de su publicación en el Boletín Oficial.

Los Responsables y Encargados del tratamiento cuentan con el plazo máximo de UN (1) año desde la publicación de esta ley en el Boletín Oficial, para adaptarse a las obligaciones contenidas en ella. A requerimiento y en casos excepcionales con motivos debidamente fundados, la Autoridad de aplicación podrá conceder a los Responsables y Encargados del tratamiento una prórroga del plazo.

En dicho plazo, conservarán plena vigencia las leyes Nros. 25.326 y 26.343 sus normas reglamentarias y las demás disposiciones que hubieran sido dictadas por la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES y/o la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA.

Comentario:

La Argentina cuenta con una ley de Protección de Datos Personales desde el año 2000 y ha sido pionera en la región sobre la materia. En ese marco, el país cuenta con trayectoria institucional en relación a la aplicación de este tipo de regulaciones que permite considerar su aplicación en un (1) año. Asimismo, el Anteproyecto establece una instancia de prórroga para aquellos responsables que lo requieran.

Conforme a las inquietudes manifiestas por la comisión, en relación al plazo para la vigencia de la Ley, se consideró que este podría ser extendido pero limitando las instancias de prórroga a efecto de unificar la vigencia del plazo de la ley a nivel federal. Para ello, se incorpora la obligación de que los Responsables y Encargados del tratamiento deban expresar los motivos debidamente fundados para hacer efectivo los pedidos de extensión de plazos para el cumplimiento de la Ley.

2.11. Jurisdicción

ARTÍCULO 75.- Orden público. Las normas de la presente ley son de orden público y de aplicación en todo el territorio nacional.

Comentario:

Considerando que este Anteproyecto regula en materia de Derechos Humanos, conforme a los establecido en los convenios internacionales a los que el país ha adherido, como es el Convenio para la Protección de las Personas en lo que respecta al Tratamiento automatiza de Datos Personales, la nueva propuesta establece que las disposiciones del Anteproyecto de Protección de Datos Personales deben ser de orden público y aplicar de manera obligatoria en todo el territorio de la República Argentina.

2.12. Consejo Federal para la Transparencia y Protección de Datos Personales

ARTÍCULO 76.- Consejo Federal para la Transparencia y Protección de Datos Personales. Modificase el Artículo 29 de la Ley 27.275 Derecho de Acceso a la Información Pública en los siguientes términos:

ARTÍCULO 29.- Consejo Federal para la Transparencia y Protección de Datos Personales. Créase el Consejo Federal para la Transparencia y Protección de Datos Personales, como organismo interjurisdiccional de carácter permanente, que tiene por objeto la cooperación técnica y la concertación de políticas en materia de transparencia, acceso a la información pública y protección de datos personales.

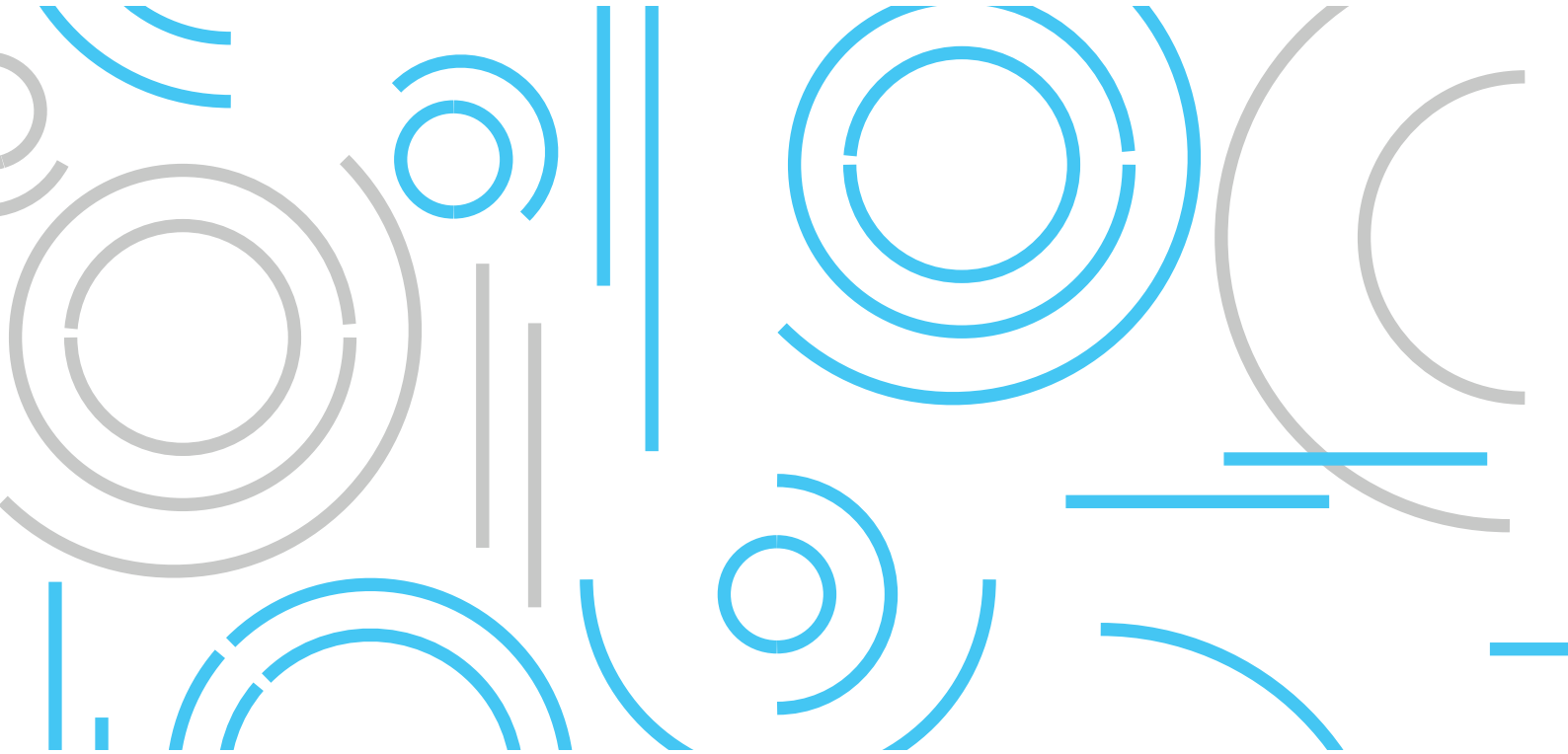
El Consejo Federal para la Transparencia y Protección de Datos Personales tiene su sede en la Agencia de Acceso a la Información Pública, de la cual recibe apoyo administrativo y técnico para su funcionamiento.

El Consejo Federal para la Transparencia y Protección de Datos Personales está integrado por un (1) representante de cada una de las provincias y un (1) representante de la Ciudad Autónoma de Buenos Aires, que deben ser los funcionarios de más alto rango en materia de transparencia activa y protección de datos personales. El Consejo Federal para la Transparencia y Protección de Datos Personales debe ser presidido por la autoridad de la Agencia de Acceso a la Información Pública y Protección de Datos Personales, quien debe convocar semestralmente a reuniones en donde se debe evaluar el grado de avance en materia de transparencia activa, acceso a la información y protección de datos personales en cada una de las jurisdicciones".

Comentario:

Fruto del debate por el Anteproyecto de Protección de Datos Personales llevado a cabo desde la comisión de Gobernanza de datos y protección de la privacidad surge la necesidad de plantear dentro de la propuesta legislativa una instancia federal para la coordinación y la concertación de políticas en materia de protección de datos personales.

Por ello, en su Artículo 76, el anteproyecto modifica el Artículo 29 de la Ley 27.275 estableciendo la creación del Consejo Federal para la Transparencia y Protección de Datos Personales. El mismo tendrá como objeto la cooperación técnica y la concertación de políticas en materia de transparencia, acceso a la información pública y protección de datos personales.



Consejo Federal
para la Transparencia

AAIP
Transpa rencia
Acceso a la Información Pública
Protección de Datos Personales

Argentina
Presidencia