CUADRO COMPARATIVO

Ley 25.326
de Protección de Datos Personales

—

Mensaje 147/2018
Proyecto de Ley de Protección de Datos Personales

AGENCIA DE ACCESO A LA
INFORMACIÓN PÚBLICA

Introducción

La protección de los datos personales se encuentra explícitamente garantizada en nuestro país a través de la acción de habeas data prevista en el artículo 43, tercer párrafo, de la Constitución Nacional, acción que fue incorporada en oportunidad de la reforma constitucional del año 1994. Posteriormente, se sancionó la Ley Nº 25.326 de Protección de Datos Personales, norma de orden público que regula los principios aplicables en la materia, así como también el procedimiento de la acción de habeas data. La mencionada ley fue sancionada en octubre del 2000 y entró en vigencia al año siguiente.

No se puede objetar que la tecnología ha evolucionado en los últimos diecisiete años a un ritmo vertiginoso, impactando en gran medida en la protección de los datos personales. Basta señalar que, por ejemplo, Facebook surgió en 2004 y Dropbox en 2007 para darse cuenta que el escenario en el que se sancionó la Ley Nº 25.326 cambió radicalmente. Esta nueva realidad de la tecnología ha traído enormes desafíos en el campo del ejercicio de los derechos. Los beneficios son innegables, pero también lo son las nuevas potenciales vulneraciones a la privacidad.

Por otro lado, actualmente se presenta un nuevo contexto regulatorio internacional en esta materia, especialmente a raíz de la adopción del Reglamento General de Protección de Datos (RGPD) que entró en vigencia el 25 de mayo del presente año y que se prevé tendrá impacto en la Argentina como parte de la comunidad internacional.

Ante este escenario, la entonces Dirección Nacional de Protección de Datos Personales (DNPDP), dependiente del Ministerio de Justicia y Derechos Humanos, tomó la iniciativa de elaborar un proyecto de ley de protección de datos personales para reformar la ley vigente. El desafío de esta tarea consistió en elaborar una nueva normativa destinada a proteger los datos personales y la privacidad de las personas, sin ser un obstáculo para la innovación y el desarrollo tecnológico y que, además, cumpliera con estándares internacionales.

La norma proyectada es el resultado de un proceso que duró más de dos años, llevado a cabo en el marco del programa "Justicia 2020", en el que intervinieron múltiples actores interesados en la materia, provenientes del sector privado, del ámbito académico y de la sociedad civil. Definitivamente, la sanción de este proyecto logrará alinear a la Argentina con las legislaciones más modernas en el mundo en materia de protección de datos personales y brindar respuesta a los desafíos presentados por el uso de nuevas tecnologías en la era digital.

El proyecto de ley garantiza adecuadamente los derechos de los titulares de los datos, aclara cuáles son las bases legales para el tratamiento de datos (incorporando al interés legítimo del responsable del tratamiento, entre otras bases legales, y alejándose de la ley vigente que únicamente contempla al consentimiento del titular de los datos) y genera obligaciones a los responsables del tratamiento de datos que son consistentes con el objeto de la norma proyectada: la protección integral de los datos personales a fin de garantizar el ejercicio pleno de los derechos de sus titulares.

En la elaboración de la norma proyectada se ha seguido de cerca la tendencia internacional en la materia, estableciendo que la normativa se aplicará en distintos supuestos, aun cuando, bajo ciertas condiciones, los responsables de tratar los datos no se encuentren

en territorio nacional. Por otra parte, se dispone que la aplicación de la ley no podrá afectar al tratamiento de datos que realicen los medios de comunicación en el ejercicio de la libertad de expresión, específicamente, remarcando en relación al derecho de supresión, que este derecho no procederá cuando el tratamiento de datos persiga un fin público o sea necesario para ejercer el derecho a la libertad de expresión e información.

Asimismo, el proyecto incorpora obligaciones a los responsables del tratamiento no contempladas en la ley vigente, entre otras: la obligación de notificar incidentes de seguridad; la obligación de realizar una evaluación del impacto relativa a la protección de los datos personales cuando sea probable que entrañe un alto riesgo de afectación a los derechos de los titulares de los datos; la obligación de adoptar medidas para el cumplimiento de la ley que sean proporcionales a las modalidades y finalidades del tratamiento de datos, su contexto, el tipo y categoría de datos tratados, y el riesgo que el referido tratamiento pueda acarrear sobre los derechos de su titular (lo que en el derecho comparado se denomina, principio de responsabilidad demostrada o proactiva, como fuera denominado en el proyecto). Además, se crea la figura del delegado de protección de datos cuya designación es obligatoria para algunos casos específicamente definidos: tratamiento de datos por parte de autoridades u organismos públicos, tratamiento de datos sensibles como parte de la actividad principal del responsable o encargado del tratamiento, y tratamiento de datos a gran escala.

Por otro lado, el proyecto de ley recepta derechos de los titulares de los datos que hasta ahora no habían sido reconocidos, como: el derecho a la portabilidad de datos; el derecho de los titulares de los datos a oponerse a ser objeto de una decisión basada única mente en el tratamiento automatizado de datos; y el derecho, bajo ciertas circunstancias, a solicitar la supresión de sus datos personales de las bases de datos, aclarándose, como fuera mencionado precedentemente, que la supresión no procede cuando el tratamiento de datos sea necesario para ejercer el derecho a la libertad de expresión e información. A su vez, y en este mismo sentido, se incorporan parámetros especiales para el tratamiento de datos de niñas, niños y adolescentes, resaltando la importancia que para ello tiene el respeto a la Convención sobre los Derechos del Niño.

Por último, cabe destacar que se designa a la Agencia de Acceso a la Información Pública (AAIP), conforme los términos del artículo 19 de la Ley Nº 27.275, sustituido por el artículo 11 del Decreto Nº 746/17, como la autoridad de control de la ley de protección de datos personales, siendo la AAIP un ente autárquico con autonomía funcional en el ámbito de la Jefatura de Gabinete de Ministros. Este diseño institucional tiende a superar los problemas generados a raíz de las observaciones efectuadas por el Poder Ejecutivo Nacional ("veto parcial") de los puntos 2 y 3 del artículo 29 de la vigente Ley Nº 25.326 al momento de su promulgación, dispuesta con la salvedad de las partes observadas mediante el Decreto Nº 995 del 30 de octubre de 2000. Este diseño institucional cumple con los estándares internacionales que requieren de autoridades de control cuya actuación esté dotada de garantías que permitan su independencia.

Ley Nº 25.326

Definiciones
ARTÍCULO 2 – Definiciones.

- Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

- Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Proyecto de Ley

Definiciones
ARTÍCULO 2 – Definiciones.

- Datos personales: información de cualquier tipo referida a personas humanas determinadas o determinables, inclusive los datos biométricos. Se entenderá por determinable la persona que pueda ser identificada mediante algún identificador o por uno o varios elementos característicos de la identidad física, fisiológica, genética (datos genéticos), psíquica, económica, cultural o social de dicha persona. No será considerada persona determinable cuando, para lograr su identificación, se requiera la aplicación de medidas o plazos desproporcionados o inviables. Se entenderá por datos biométricos aquellos datos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identificación única. Se entenderá por datos genéticos los relativos a las características genéticas heredadas o adquiridas de una persona humana que proporcionen una información sobre su fisiología o salud, obtenidos en particular del análisis de una muestra biológica.

- Datos sensibles: datos personales que afectan la esfera íntima de su titular con potencialidad de originar una discriminación ilícita o arbitraria, en particular, los que revelan origen racial o étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, participación o afiliación en una organización sindical o política, información referente a la salud, preferencia o vida sexual.

Categoría de datos y condiciones especiales que aplican a los datos sensibles
ARTÍCULO 7º - Categoría de datos.

1. Ninguna persona puede ser obligada a proporcionar datos sensibles.
2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.
3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.
4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

Categoría de datos y bases legales para su tratamiento
ARTÍCULO 16 – Tratamiento de datos sensibles.

Se prohíbe el tratamiento de datos sensibles, excepto cuando:
a. El titular de los datos haya dado su consentimiento expreso a dicho tratamiento, salvo en los casos en que por ley no sea requerido el otorgamiento de dicha autorización;
b. Sea necesario para salvaguardar el interés vital del titular de los datos y éste se encuentre física o legalmente incapacitado para prestar el consentimiento y sus representantes legales no lo puedan realizar en tiempo oportuno;
c. Sea efectuado por establecimientos sanitarios públicos o privados o por profesionales vinculados a la ciencia de la salud en el marco 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;
d. Se realice en el marco de las actividades legítimas que realice 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;
e. Se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
f. Tenga una finalidad histórica, estadística o científica. En estos DOS (2) últimos casos, debe adoptarse un procedimiento de disociación de datos;
g. Se refiera a datos personales que el interesado haya hecho manifiestamente públicos;
h. Sea 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 y Protección Social;
i. Sea necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios;
j. Se realice en el marco de asistencia humanitaria en casos de desastres naturales.

ARTÍCULO 8º - Datos relativos a la salud.

Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional.

ARTÍCULO 17 - Tratamiento de antecedentes penales y contravencionales.

El tratamiento de datos relativos a antecedentes penales o contravencionales con el objeto de brindar informes a terceros sólo puede ser realizado por parte de las autoridades públicas competentes o bajo su supervisión.
El empleador que conserve un certificado, documento o información de antecedentes penales o contravencionales de sus empleados no puede cederlo a terceros, salvo con el consentimiento expreso del titular de los datos.

ARTÍCULO 18 – Tratamiento de datos de niñas, niños y adolescentes.

En el tratamiento de datos personales de una niña, niño o adolescente, se debe privilegiar la protección del interés superior de éstos, conforme a la CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO y demás instrumentos internacionales que busquen su bienestar y protección integral.
Es válido el consentimiento de una niña, niño o adolescente cuando se aplique 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 lícito si el menor de edad tiene como mínimo TRECE (13) años. Si la niña o niño es menor de TRECE (13) años, tal tratamiento únicamente se considera lícito si el consentimiento fue otorgado por el titular de la responsabilidad parental o tutela sobre la niña o niño, y sólo en la medida en que se dio o autorizó.
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 tutela sobre la niña, niño o adolescente, teniendo en cuenta sus posibilidades para hacerlo.

Principios relativos al tratamiento de los datos personales

Ley Nº 25.326

Obligación de registración y licitud de las bases de datos
ARTÍCULO 3° - Archivos de datos - Licitud.

La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia.
Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.

Calidad de los datos
ARTÍCULO 4° - Calidad de los datos.

1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

Proyecto de Ley

Principio de lealtad y transparencia. No obligación de registración - Principio de responsabilidad demostrada
ARTÍCULO 5º - Principio de lealtad y transparencia.

Los datos personales deben ser tratados de manera leal y transparente. El tratamiento se considera leal cuando el responsable se abstiene de tratar los datos personales a través de medios engañosos o fraudulentos.

ARTÍCULO 10 - Principio de responsabilidad proactiva.

El responsable o encargado del tratamiento debe adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar un tratamiento adecuado de los datos personales y el cumplimiento de las obligaciones dispuestas por la presente Ley, y que le permitan demostrar a la autoridad de control su efectiva implementación.

Principios de finalidad, de minimización, de exactitud y plazo de conservación
ARTÍCULO 6º - Principio de finalidad.

Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no deben ser tratados de manera incompatible con dichos fines. No se considerarán incompatibles con los fines iniciales tanto el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos, como tampoco el tratamiento de datos con fines que pudieron ser, de acuerdo al contexto, razonablemente presumidos por el titular de los datos.

2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.
3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.
4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.
5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.
6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.
7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

ARTÍCULO 7º - Principio de minimización de datos.

Los datos personales deben ser tratados de manera que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que fueron recolectados.

ARTÍCULO 8º - Principio de exactitud.

Los datos personales deben ser tratados de modo que sean exactos y completos. Si fuera necesario adecuarlos, se adoptarán todas las medidas razonables para que se supriman o rectifiquen.

ARTÍCULO 9º - Plazo de conservación.

Los datos personales no deben ser mantenidos más allá del tiempo estrictamente necesario para el cumplimiento de la finalidad del tratamiento. Los datos personales pueden conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone la presente Ley a fin de proteger los derechos del titular de los datos.

Consentimiento
ARTÍCULO 5° - (Consentimiento).

1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.
El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.
2. No será necesario el consentimiento cuando:
a) Los datos se obtengan de fuentes de acceso público irrestricto;
b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;
d) Deriven de una relación contractual, científica o profesional del titular

Bases legales para el tratamiento de datos personales
ARTÍCULO 11 - Licitud del tratamiento de datos.

El tratamiento de datos es lícito sólo si se cumple al menos UNA (1) de las siguientes condiciones:
a. El titular de los datos dé su consentimiento para el tratamiento de sus datos para uno o varios fines específicos conforme lo dispuesto en los artículos 12, 13 y 14 de la presente;
b. El tratamiento de datos se realice sobre datos que figuren en fuentes de acceso público irrestricto;
c. El tratamiento de datos se realice en ejercicio de funciones propias de los poderes del Estado y sean necesarios para el cumplimiento estricto de sus competencias;
d. El tratamiento de datos sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
e. El tratamiento de datos derive de una relación jurídica entre el titular de los datos y el responsable del tratamiento, y resulte necesario para su desarrollo o cumplimiento;
f. El tratamiento de datos 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 el titular de los datos esté física o jurídicamente incapacitado para dar su consentimiento;
g. El tratamiento de datos sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos del titular de los datos, en particular cuando el titular sea un niño, niña o adolescente.

ARTÍCULO 12 - Consentimiento.

El tratamiento de datos, en cualquiera de sus formas, requiere del consentimiento libre e informado de su titular para una o varias finalidades específicas.
El consentimiento puede ser obtenido de forma expresa o tácita.
La forma del consentimiento depende de las circunstancias, el tipo de dato personal y las expectativas razonables del titular de los datos.

de los datos, y resulten necesarios para su desarrollo o cumplimiento;
e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.

El consentimiento expreso, de acuerdo a las circunstancias particulares del tratamiento de datos del que se trate, puede ser obtenido por escrito, verbalmente, por medios electrónicos, así como por cualquier forma similar que la tecnología permita brindar.
Para el tratamiento de datos sensibles se requiere el consentimiento expreso, salvo las excepciones establecidas por ley.
El consentimiento tácito es admitido cuando surja de manera manifiesta del contexto del tratamiento de datos y la conducta del titular de los datos sea suficiente para demostrar la existencia de su autorización. Es admisible únicamente cuando los datos requeridos sean necesarios para la finalidad que motiva la recolección y se haya puesto a disposición del titular de los datos la información prevista en el artículo 15, sin que éste manifieste su oposición. El tratamiento de datos ulterior debe ser compatible con las finalidades manifiestas que surgen del contexto que originó la recolección. En ningún caso procede para el tratamiento de datos sensibles.
En todos los casos, el responsable del tratamiento tiene la carga de demostrar que el titular de los datos consintió el uso de sus datos personales.

ARTÍCULO 13 - Revocación del consentimiento.

El consentimiento puede ser revocado en cualquier momento. Dicha revocación no tiene efectos retroactivos. El responsable del tratamiento está obligado a facilitar la revocación mediante mecanismos sencillos, gratuitos y, al menos, de la misma forma por la que obtuvo el consentimiento.

ARTÍCULO 14 - Excepciones al consentimiento previo.

No es necesario el consentimiento para el tratamiento de datos cuando se trate de listados cuyos datos se limiten a nombre y apellido, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento, domicilio y correo electrónico, ni para el tratamiento de la información crediticia en los términos del Capítulo 6.

Información al titular de los datos
ARTÍCULO 6° - Información.

Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:
a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;
b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;
c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;
d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;
e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Información al titular de los datos
ARTÍCULO 15 - Información al titular de los datos.

El responsable del tratamiento debe brindar al titular de los datos, antes de la recolección, al menos, la siguiente información:
a. Las finalidades del tratamiento de datos a las que se destinarán los datos personales recolectados;
b. La identidad y los datos de contacto del responsable del tratamiento;
c. Los medios para ejercer los derechos previstos en esta Ley;
d. En su caso, las cesiones o transferencias internacionales de datos que se efectúen o se prevea efectuar;
e. El carácter obligatorio o facultativo de proporcionar los datos personales y las consecuencias de proporcionarlos, o de la negativa a hacerlo, o de hacerlo en forma incompleta o defectuosa;
f. El derecho del titular de los datos a revocar el consentimiento;
g. El derecho a presentar una denuncia, a iniciar el trámite de protección de datos personales ante la autoridad de control, o a ejercer la acción de habeas data en caso de que el responsable o el encargado del tratamiento incumpla con la presente Ley.

Seguridad de los datos
ARTÍCULO 9° - (Seguridad de los datos).

1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

Principio de seguridad de los datos y notificación de incidentes de seguridad
ARTÍCULO 19 - Principio de seguridad de los datos personales.

El responsable del tratamiento y, en su caso, el encargado, deben adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.
El responsable del tratamiento debe adoptar las medidas de seguridad aplicables a los datos personales que trate, considerando, al menos, los siguientes factores:
a. El riesgo inherente por el tipo de dato personal;
b. El carácter sensible de los datos personales tratados;
c. El desarrollo tecnológico;
d. Las posibles consecuencias de un incidente de seguridad para los titulares de los datos;
e. Los incidentes de seguridad previos ocurridos en los sistemas de tratamiento.

ARTÍCULO 20 - 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 control sin dilación indebida y, de ser posible, dentro de las SETENTA Y DOS (72) horas de haber tomado conocimiento del incidente, a menos que sea improbable que dicho incidente de seguridad constituya un riesgo para los derechos de los titulares de los datos. Si la notificación a la autoridad de control no tiene lugar en el plazo de SETENTA Y DOS (72) horas, deberá ir acompañada de indicación de los motivos de la dilación.
De igual manera, el responsable del tratamiento también debe informar al titular de los datos sobre el incidente de seguridad ocurrido, en un lenguaje claro y sencillo, cuando sea probable que entrañe altos riesgos a sus derechos.
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.
El responsable del tratamiento debe documentar todo incidente de seguridad que ponga en alto riesgo los derechos de los titulares de los datos personales 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.

Confidencialidad
ARTÍCULO 10 - Deber de confidencialidad.

1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Confidencialidad
ARTÍCULO 21 - Deber de confidencialidad.

El responsable del tratamiento, el encargado y las demás personas que intervengan en cualquier fase del tratamiento de datos están obligados a la confidencialidad respecto de los datos personales. Tal obligación subsiste aun después de finalizada su relación con el titular de los datos, el responsable o el encargado del tratamiento, según corresponda.
El obligado puede ser relevado del deber de confidencialidad por resolución judicial.

Cesión de datos personales

Ley Nº 25.326

Cesión
ARTÍCULO 11. - (Cesión).

1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.
2. El consentimiento para la cesión es revocable.
3. El consentimiento no es exigido cuando:
a) Así lo disponga una ley;
b) En los supuestos previstos en el artículo 5° inciso 2;
c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;

Proyecto de Ley

Cesión*

**Al ser la cesión un tipo de tratamiento, no había necesidad de incorporar un artículo específico que estableciera las condiciones para realizar una cesión, puesto que le aplican las mismas condiciones que a cualquier otro tipo de tratamiento (art. 11 – licitud del tratamiento), a excepción de la responsabilidad solidaria.*

ARTÍCULO 22 - Cesión.

Cuando 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 responsable cedente. Ambos responden por la observancia de aquéllas ante la autoridad de control y el titular de los datos de que se trate. En cualquier caso, podrán ser eximidos total o parcialmente de responsabilidad si demuestran que no se les puede imputar el hecho que ha producido el daño.

d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;
e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.
4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.

Ley Nº 25.326

Transferencia internacional de datos personales

ARTÍCULO 12 - Transferencia internacional.

1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.
2. La prohibición no regirá en los siguientes supuestos:
a) Colaboración judicial internacional;
b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior;
c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;

Proyecto de Ley

Transferencia internacional de datos personales
ARTÍCULO 23 - Transferencia internacional.

Toda transferencia internacional de datos personales es lícita si se cumple al menos UNA (1) de las siguientes condiciones:
a. Cuente con el consentimiento expreso del titular de los datos;
b. El país u organismo internacional o supranacional receptor proporcione un nivel de protección adecuado;
c. Se encuentre prevista en una ley o tratado en los que la REPÚBLICA ARGENTINA sea parte;
d. Sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
e. Sea efectuada a cualquier sociedad del mismo grupo económico del responsable del tratamiento, en tanto los datos personales sean utilizados para finalidades que no sean incompatibles con las que originaron su recolección;
f. Sea necesaria en virtud de un contrato celebrado o por celebrar en interés inequívoco del titular de los datos, por el responsable del tratamiento y un tercero;
g. Sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;
h. Sea necesaria para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
i. Sea necesaria para el mantenimiento o cumplimiento de una relación jurídica entre el responsable del tratamiento y el titular de los datos;
j. Sea efectuada en los casos de colaboración judicial internacional;
k. Sea requerida para concretar transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;

d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;
e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

Decreto Nº 1558/01

ARTÍCULO 12 - La prohibición de transferir datos personales hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, no rige cuando el titular de los datos hubiera consentido expresamente la cesión.
No es necesario el consentimiento en caso de transferencia de datos desde un registro público que esté legalmente constituido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones legales y reglamentarias para la consulta (...).

l. Tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo, el lavado de activos, los delitos informáticos y el narcotráfico;
m. El responsable del tratamiento transferente y el destinatario adopten mecanismos de autorregulación vinculante, siempre y cuando éstos sean acordes a las disposiciones previstas en esta Ley;
n. Se realice en el marco de cláusulas contractuales que contengan mecanismos de protección de los datos personales acordes con las disposiciones previstas en la presente Ley.
El receptor de los datos personales asume las mismas obligaciones que corresponden al responsable del tratamiento que transfirió los datos personales.

ARTÍCULO 24 - Carácter adecuado del país u organismo receptor.

El nivel de protección proporcionado por un país u organismo internacional o supranacional será evaluado por la autoridad de control, a pedido de parte interesada o de oficio y atendiendo a todas las circunstancias que concurran en una transferencia internacional; en particular, las normas de derecho, generales o especiales, vigentes en el país u organismo internacional o supranacional de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad que resulten aplicables.

ARTÍCULO 25 - Prueba del cumplimiento de las obligaciones en materia de transferencias internacionales.

A efectos de demostrar que la transferencia internacional se ha realizado conforme a lo que establece la presente Ley, la carga de la prueba recae, en todos los casos, en el responsable del tratamiento que transfiere.

Ley Nº 25.326

Derechos del titular de los datos personales
ARTÍCULO 13 - Derecho de Información.

Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables.
El registro que se lleve al efecto será de consulta pública y gratuita.

ARTÍCULO 14 - Derecho de acceso.

1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.
2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente.

Proyecto de Ley

Derechos del titular de los datos personales
ARTÍCULO 27 - Derecho de acceso.

El titular de los datos, previa acreditación de su identidad, tiene el derecho de solicitar y obtener el acceso a sus datos personales que sean objeto del tratamiento.

ARTÍCULO 28 - Contenido de la información.

La información debe ser suministrada en forma clara, exenta de codificaciones y, en su caso, acompañada de una explicación de los términos que se utilicen, en lenguaje accesible al conocimiento medio de la población, y debe versar sobre:
a. Las finalidades del tratamiento de datos;
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, en particular cuando se trate de una transferencia internacional;
d. El plazo previsto de conservación de los datos personales o, de no ser ello posible, los criterios utilizados para determinar este plazo;
e. La existencia del derecho a solicitar del responsable del tratamiento la rectificación, supresión de datos personales o a oponerse a dicho tratamiento;
f. El derecho a iniciar un trámite de protección de datos personales ante la autoridad de control;
g. Cuando los datos personales no se hayan obtenido del titular de los datos, cualquier información disponible sobre su origen;
h. La existencia de decisiones automatizadas, incluida la elaboración de perfiles a que se refiere el artículo 32 y, al menos en tales casos, información significativa sobre

Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley.
3. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.
4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.

ARTÍCULO 15 - Contenido de la información.

1. La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen.
2. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el 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 cuando se vinculen con el titular de los datos.
La información, a opción del titular de los datos, puede suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

ARTÍCULO 29 - Derecho de rectificación.

El titular de los datos tiene el derecho a obtener del responsable del tratamiento la rectificación de sus datos personales, cuando éstos resulten ser inexactos, falsos, errados, incompletos o no se encuentren 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 QUINTO (5°) día hábil de haber tomado conocimiento efectivo del error o la desactualización. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable del tratamiento debe bloquear el dato, o bien consignar, al proveer información relativa a éste, la circunstancia de que se encuentra sometido a revisión.

ARTÍCULO 30 - Derecho de oposición.

El titular de los datos puede oponerse al tratamiento de sus datos, o de una finalidad específica de éste, cuando no haya 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.

ARTÍCULO 31 - Derecho de supresión.

El titular de los datos tiene derecho a solicitar la supresión de sus datos personales de las bases de datos del responsable del tratamiento cuando el tratamiento no

requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.
3. La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

ARTÍCULO 16 - Derecho de rectificación, actualización o supresión.

1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.
2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.
3. El incumplimiento de esta obligación dentro del término acordado en tenga un fin público, a fin de que los datos ya no estén en su posesión y dejen de ser tratados por este último.
La supresión procede cuando:
a. Los datos personales ya no sean necesarios en relación con los fines para los que fueron recolectados;
b. El titular de los datos revoque el consentimiento en que se basa el tratamiento de datos y éste no se ampare en otro fundamento jurídico;
c. El titular de los datos haya ejercido su derecho de oposición conforme al artículo 30, y no prevalezcan 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.
La supresión no procederá 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.
La supresión tampoco procede cuando el tratamiento de datos sea necesario para ejercer el derecho a la libertad de expresión e información.

ARTÍCULO 32 - Valoraciones personales automatizadas.

El titular de los datos tiene derecho a oponerse a ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos, incluida la elaboración de perfiles, que le produzca efectos jurídicos perniciosos o lo afecte significativamente de forma negativa.
El titular de los datos no podrá ejercer este derecho si la decisión:
a. Es necesaria para la celebración o la ejecución de un contrato entre el titular de los datos y el responsable del tratamiento;
b. Está autorizada por Ley;
c. Se basa en su consentimiento expreso.
En los casos a que se refieren los incisos a) y c), el responsable del tratamiento

el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.
4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.
5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.
6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.
7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.

debe adoptar las medidas adecuadas para salvaguardar los derechos del titular de los datos.

ARTÍCULO 33 - Derecho a la portabilidad de datos personales.
Si se brindan servicios en forma electrónica que incluyan el tratamiento de datos personales, el titular de los datos tiene derecho a obtener del responsable del tratamiento una copia de los datos personales objeto de tratamiento en un formato estructurado y comúnmente utilizado que le permita su ulterior utilización. El titular de los datos puede solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible.
Este derecho no procederá cuando:
a. Su ejercicio imponga una carga financiera o técnica excesiva o irrazonable sobre el responsable o encargado del tratamiento;
b. Vulnere la privacidad de otro titular de los datos;
c. Vulnere las obligaciones legales del responsable o encargado del tratamiento; d. Impida que el responsable del tratamiento proteja sus derechos, su seguridad o sus bienes, o los derechos, seguridad y bienes del encargado del tratamiento, o del titular de los datos o de un tercero.

Ley Nº 25.326

Obligaciones del responsable y del encargado del tratamiento de datos personales
ARTÍCULO 9° - Seguridad de los datos.

1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.
2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

Proyecto de Ley

Obligaciones del responsable y del encargado del tratamiento de datos personales
ARTÍCULO 37 - Medidas para el cumplimiento de la responsabilidad proactiva.

Las medidas adoptadas para el cumplimiento de las disposiciones de la presente Ley deben ser proporcionales a las modalidades y finalidades del tratamiento de datos, su contexto, el tipo y categoría de datos tratados, y el riesgo que el referido tratamiento pueda acarrear sobre los derechos de su titular.
Deben contemplar, como mínimo:
a. La adopción de procesos internos para llevar adelante de manera efectiva las medidas de responsabilidad;
b. La implementación de procedimientos para atender el ejercicio de los derechos por parte de los titulares de los datos;
c. La realización de supervisiones o auditorías, internas o externas, para controlar el cumplimiento de las medidas adoptadas.
Las medidas deben ser aplicadas de modo que permitan su demostración ante el requerimiento de la autoridad de control.
Se debe adoptar una política de privacidad o adherirse a mecanismos de autorregulación vinculantes, que serán valorados por la autoridad de control para verificar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

ARTÍCULO 38 - Protección de datos desde el diseño y por defecto.

El responsable del tratamiento debe aplicar medidas tecnológicas y organizativas apropiadas tanto con anterioridad como durante el tratamiento de datos a fin de cumplir los principios y los derechos de los titulares de los datos establecidos en la presente Ley. Las medidas deben ser adoptadas teniendo en cuenta el estado de la

ARTÍCULO 21 - Registro de archivos de datos. Inscripción.

1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control.
2. El registro de archivos de datos debe comprender como mínimo la siguiente información:
a) Nombre y domicilio del responsable;
b) Características y finalidad del archivo;
c) Naturaleza de los datos personales contenidos en cada archivo;
d) Forma de recolección y actualización de datos;
e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;
f) Modo de interrelacionar la información registrada;
g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;
h) Tiempo de conservación de los datos;
i) Forma y condiciones en que las personas pueden acceder a los datos

tecnología, los costos de la implementación y la naturaleza, ámbito, contexto y fines del tratamiento de datos, así como los riesgos que entraña el tratamiento para el derecho a la protección de los datos de sus titulares.
El responsable 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 recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas deben garantizar en particular que, por defecto, los datos personales no sean accesibles, sin la intervención del titular de los datos, a un número indeterminado de personas humanas.

ARTÍCULO 40 - Evaluación de impacto relativa a la protección de datos personales.

Cuando el responsable del tratamiento prevea realizar algún tipo de tratamiento de datos que por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación a los derechos de los titulares de los datos amparados en la presente Ley, deberá realizar, de manera previa a la implementación del tratamiento, una evaluación del impacto relativa a la protección de los datos personales.
La evaluación de impacto relativa a la protección de los datos es obligatoria en los siguientes casos, sin perjuicio de otros que establezca la autoridad de control:
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.

ARTÍCULO 41 - Contenido de la evaluación de impacto.

La evaluación debe incluir, como mínimo:

referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.
3) Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro.
El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el capítulo VI de la presente ley.

a. Una descripción sistemática de las operaciones de tratamiento de datos previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
b. Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento de datos con respecto a su finalidad;
c. Una evaluación de los riesgos para la protección de los datos personales de los titulares de los datos a que se refiere el inciso a);
d. Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de los datos personales, y para demostrar la conformidad con la presente Ley , teniendo en cuenta los derechos e intereses legítimos de los titulares de los datos y de otras personas que pudieran verse potencialmente afectadas.

ARTÍCULO 42 - Informe previo.

El responsable del tratamiento debe informar a la autoridad de control antes de proceder al tratamiento de datos cuando una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento de datos entrañaría un alto riesgo.
El informe a la autoridad de control debe incluir, como mínimo, la siguiente información:
a. Las responsabilidades respectivas del responsable del tratamiento y los encargados del tratamiento, en particular en caso de tratamiento de datos dentro de un mismo grupo económico;
b. Los fines y medios del tratamiento previsto;
c. Las medidas y garantías establecidas para proteger los datos personales de sus titulares de conformidad con la presente Ley;
d. En su caso, los datos de contacto del Delegado de Protección de Datos;
e. La evaluación de impacto relativa a la protección de datos.
Cuando la autoridad de control considere que el tratamiento de datos previsto pueda infringir la presente Ley, iniciará el procedimiento de verificación de oficio establecido en el artículo 74.

ARTÍCULO 43.- 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. Cuando revistan el carácter de autoridades u organismos públicos;
b. Se realice tratamiento de datos sensibles como parte de la actividad principal del responsable o encargado del tratamiento;
c. Se realice tratamiento de datos a gran escala.
Cuando los responsables y encargados del tratamiento no se encuentren obligados a la designación de un Delegado de Protección de Datos de acuerdo a lo previsto en este artículo, pero decidan designarlo de manera voluntaria o por orden expresa de la autoridad de control, el Delegado de Protección de Datos designado tendrá las funciones previstas en el artículo 44.
Cuando 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 establecimiento.
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 locación de servicios. El Delegado de Protección de Datos puede ejercer otras funciones siempre que no den lugar a conflictos de intereses.
En cualquier caso, el delegado debe ejercer sus funciones sin recibir instrucciones y sólo responde ante el más alto nivel jerárquico de la organización.

ARTÍCULO 44.- 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 que tienen, derivadas de la normativa de protección de datos;
b. Promover y participar en el diseño y aplicación de una política de protección de datos que contemple los tratamientos de datos que realice el responsable o encargado del tratamiento;
c. Supervisar el cumplimiento de la presente Ley y de la política de protección de datos de un organismo público, empresa o entidad privada;
d. Asignar responsabilidades, concientizar y 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 de los datos, y supervisar luego su aplicación;
f. Cooperar y actuar como referente ante la autoridad de control para cualquier consulta sobre el tratamiento de datos efectuado por el responsable o encargado del tratamiento.

ARTÍCULO 45 - Mecanismos de autorregulación vinculantes.

La autoridad de control alentará la elaboración de mecanismos de autorregulación vinculantes que tengan por objeto contribuir a la correcta aplicación de la presente Ley, teniendo en cuenta las características específicas del tratamiento de datos que se realice, así como el efectivo ejercicio y respeto de los derechos del titular de los datos.
Los mecanismos de autorregulación vinculantes se pueden traducir en códigos de conducta, de buenas prácticas, normas corporativas vinculantes, sellos de confianza,

certificaciones u otros mecanismos que coadyuven a contribuir a los objetivos señalados.
Los responsables o encargados del tratamiento pueden adherirse, de manera voluntaria, a mecanismos de autorregulación vinculantes.
Las asociaciones u otras entidades representativas de categorías de responsables o encargados del tratamiento podrán adoptar mecanismos de autorregulación vinculantes que resulten obligatorios para todos sus miembros.
Los mecanismos de autorregulación vinculantes serán presentados a la homologación de la autoridad de control, la cual dictaminará si los mecanismos se adecuan a las disposiciones de la presente Ley y, en su caso, los aprobará o indicará las correcciones que estime necesarias para su aprobación.
Los mecanismos de autorregulación vinculantes que resulten aprobados serán registrados y dados a publicidad por la autoridad de control.

Ley Nº 25.326

ARTÍCULO 31 - Sanciones administrativas.

1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos.

2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

Proyecto de Ley

ARTÍCULO 77 - La autoridad de control podrá imponer a los responsables y encargados del tratamiento las siguientes sanciones:

a. Apercibimiento;
b. Multa de hasta el equivalente a QUINIENTOS (500) Salarios Mínimos Vitales y Móviles vigentes al momento de la imposición de la sanción;
c. Suspensión de las actividades relacionadas con el tratamiento de datos hasta por un término de SEIS (6) meses; en el acto de suspensión se indicarán las medidas correctivas que deberán adoptarse;
d. Cierre temporal de las operaciones relacionadas con el tratamiento de datos una vez transcurrido el término de suspensión sin que se hubieren adoptado las medidas correctivas ordenadas por la autoridad de control;
e. Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

En todos los casos la autoridad de control dará a publicidad la resolución en su sitio web, y ordenará su publicación en el sitio web del responsable, a su costa.

Al disponer la suspensión o cierres previstos en los incisos c), d) y e) la autoridad de control podrá requerir al juez competente que, de manera temporal o definitiva, ordene el retiro, bloqueo, suspensión y/o inhabilitación del acceso a los datos personales a los que los responsables del tratamiento den acceso, interconecten, transmitan o direccionen, almacenen, alojen, intermedien, enlacen o busquen, que lesionen derechos legalmente reconocidos. A tal efecto, la autoridad de control deberá precisar, de acuerdo a lo informado por el titular de los datos, el enlace en el que se encuentren alojados los datos personales o los procedimientos para acceder a aquél.

En ningún caso, estas medidas podrán afectar el derecho a la libertad de expresión e información

ARTÍCULO 78 - Incumplimiento de autoridad pública.

Las sanciones indicadas en el artículo anterior sólo se aplican a las personas de naturaleza privada. En caso de que la autoridad de control advierta un presunto incumplimiento de las disposiciones de la presente Ley por parte de una autoridad pública, remitirá la actuación a la autoridad que corresponda para que inicie la investigación respectiva.

ARTÍCULO 79 - Gradación. Las sanciones a las que se refiere el artículo 77 se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:

a. La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente Ley;
b. El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;
c. La reincidencia en la comisión de la infracción;
d. La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la autoridad de control;
e. El incumplimiento de los requerimientos u órdenes impartidas por la autoridad de control;
f. El reconocimiento o aceptación expreso que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.
La designación voluntaria de un Delegado de Protección de Datos, la adopción de mecanismos de autorregulación vinculantes, la realización de una evaluación de impacto en los términos del artículo 40 y la notificación oportuna de incidentes de seguridad serán merituados como atenuantes de la sanción que corresponda, sin perjuicio de otros que pueda considerar la autoridad de control.

AGENCIA DE ACCESO A LA
INFORMACIÓN PÚBLICA

www.argentina.gob.ar/aaip

@AAIPargentina