Algunas consideraciones sobre la nueva ley de protección de datos personales (Ley 18.331)

Nuestro país cuenta a partir de agosto de 2008 con una nueva ley de protección de datos personales, que incorpora y profundiza lo que establecía la anterior ley en esta materia (Ley 17.838) así como también la deroga.
Los motivos que llevaron a la promulgación de esta nueva ley pueden resumirse principalmente en tres:

1. La adecuación de nuestro marco regulatorio a los estándares exigidos internacionalmente en el tratamiento y protección de datos personales.
2. A través de lo anterior, la captación de inversores en los sectores de servicios y tecnológicos.
3. La protección del derecho a la privacidad y al adecuado tratamiento de los datos personales.

Definiciones

El artículo 1° de la ley consagra la protección de los datos personales como inherente a la persona humana y por tanto comprendido en el artículo 71 de la Constitución, extendiendo este derecho –en cuanto corresponda- a las personas jurídicas (Art. 2°). Esto significa que este derecho se eleva al mismo nivel de los más importantes derecho de la persona como la vida, la propiedad o la libertad.

Es de vital importancia tener presente cuáles son las bases de datos alcanzadas por la presente ley, y cuáles no. Esta determinación está dada por el artículo 3° de la ley en estudio el que establece: "*El régimen de la presente ley será de aplicación a los **datos personales** registrados en **cualquier soporte** que los haga **susceptibles de tratamiento**, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado.*"

Lo anterior requiere para su mejor comprensión, la definición de ciertos conceptos manejados por la ley, y que ella misma enumera en su artículo 4°:

- Base de datos: El conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.
- Dato personal: Información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables.
- Tratamiento de datos: Operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos

personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Sin perjuicio de lo anterior, el artículo 3° de la ley establece las excepciones, esto es las bases de datos que no estarán comprendidas en la presente ley. Estas son:

a) Las mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b) Las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.
c) Las bases de datos creadas y reguladas por leyes especiales.

Por tanto, podemos concluir que la ley será aplicable a todos aquellos conjuntos organizados de datos mantenidos por personas físicas o jurídicas referidos a otras personas que pudieran ser procesados, cedidos, transferidos, etc. A los efectos prácticos del presente informe, es posible decir que las únicas bases de datos que no estarían alcanzadas por la presente ley serían las domésticas, las que uno mantiene en su hogar o en su ámbito privado y que no tienen fines comerciales o profesionales.

Principios

El responsable de la base de datos, esto es, el propietario de la base de datos o quien decida sobre la finalidad, contenido o uso del tratamiento que a esos datos se les de, deberá adecuar su actuación a determinados principios legales enumerados y definidos en los artículos 5° y siguientes.

1) Principio de legalidad: Este principio abarca dos aspectos. Por un lado, establece que lícitas serán las bases de datos debidamente inscriptas de acuerdo a lo que se dirá, y en las que en su operación se observe lo establecido en la ley. Por otro lado, también se establece que las bases de datos no podrán tener fines ilícitos o contrarios a la moral.
2) Principio de veracidad: La ley preceptúa que los datos recabados deberán ser veraces, adecuados y no excesivos para el fin para el que se hubieran obtenido, y que la recolección de esos datos no se podrá hacer por medios desleales, abusivos o ilícitos. También impone al responsable de su tratamiento la obligación de suprimir, sustituir o completar aquellos datos que llegue a su conocimiento son inexactos o incompletos.
3) Principio de finalidad: Establece que los datos obtenidos no podrán ser utilizados para fines distintos para aquellos para los que fueron

recabados. Esto es, si la persona facilitó sus datos para la obtención de una tarjeta de crédito, ellos no podrán ser utilizados para enviarle publicidad o mailings. También se impone la obligación de eliminar todos aquellos datos que hubieran dejado de ser necesarios o pertinentes a los efectos para los cuales se hubieren recabado.

4) Previo consentimiento informado: El tratamiento de los datos será lícito cuando el titular de los mismos hubiere dado su consentimiento libre, previo, expreso e informado, y el que deberá constar por escrito. No será necesario el previo consentimiento escrito de la persona cuando:
    - Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación.
    - En caso de personas físicas, los datos recolectados se limiten a nombre, documento de identidad, nacionalidad, domicilio y fecha de nacimiento; y en el caso de personas físicas a la razón social, nombre de fantasía, RUT, domicilio, teléfono e identidad de sus autoridades.
    - Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.
    - Se recaben en el ejercicio de las funciones propias de los poderes del Estado o en virtud de una obligación legal.
    - Su recolección se realice para el uso exclusivo personal o doméstico.
5) Principio de seguridad de los datos: Se deberán adoptar las medidas necesarias para garantizar la seguridad y confidencialidad de los datos, evitando su adulteración, pérdida, consulta o tratamiento no autorizado. No se podrán almacenar datos en bases que no reúnan condiciones técnicas de integridad y seguridad.
6) Principio de reserva: Todos aquellos que legítimamente obtengan información de bases de datos, o tuvieran acceso a ellas, deberán guardar reserva sobre los datos obtenidos o llegados a su conocimiento. En algunos casos, la difusión de la información obtenida puede dar lugar a la aplicación del artículo 302 del Código Penal (Revelación de Secreto Profesional).

Derechos de los titulares de los datos y las obligaciones correlativas impuestas a quienes recaben o traten dichos datos

La Ley 18.331 establece en su capítulo III una serie de derechos de las personas al momento de la recolección de sus datos, su tratamiento y su difusión. Evidentemente, los derechos otorgados a las personas implican obligaciones para las personas u organizaciones que recaban, tratan o trasmiten esos datos.

En primer lugar se establece la obligación, previa a la recolección de los datos, de informar a su titular en forma expresa, precisa e inequívoca la finalidad para la que serán tratados y quienes pueden ser sus detinatarios; la existencia de la base de datos, así como la identidad y domicilio de su responsable; el carácter obligatorio o facultativo de las respuestas al cuestionario (especialmente en lo relativo a datos sensibles –religión, orientación sexual, preferencia política-); las consecuencias de proporcionar o no los datos; y la posibilidad del titular de acceder a esos datos, obtener su rectificación o su supresión.

Otro derecho consagrado al titular de los datos es el de obtener acceso a los mismos, y la obligación de quien trate dichos datos de proporcionar a pedido del titular el total de la información que sobre él existan en esa base de datos. El titular de los datos tendrá el derecho de solicitar la rectificación, actualización, inclusión o supresión de datos en caso que los mismos sean erróneos, falsos o incompletos.

Por su parte, los artículos 16 y 17 de la ley en estudio consagran dos importantes y significativos derechos para las personas cuyos datos sean tratados.

En primer lugar, el artículo 16 consagra el derecho de la persona a impugnar la valoración personal que de ella se haga exclusivamente en virtud de los datos existentes en la base de datos. Indica este artículo que la persona tendrá derecho a no verse sometida a una decisión con efectos jurídicos que lo afecte de manera significativa basada simplemente en la evaluación de datos. Aspectos de la personalidad de una persona tales como su rendimiento laboral, su crédito, su fiabilidad su conducta entre otros, no podrán ser evaluados tomando como base al tratamiento automatizado o no de los datos existentes en las bases, y un acto administrativo o decisión privada cuyo único fundamento fuera ese tratamiento podrá ser impugnado por el sujeto.

Por último, el artículo 17 regula la comunicación de los datos tratados donde se indica que para dicha operación se deberá contar con el consentimiento previo y escrito del titular de los datos, así como también los casos excepcionales donde ese

consentimiento previo no será necesario, y las obligaciones del receptor. Por la complejidad que implica este punto, su estudio en profundidad será realizado más adelante.

Datos especialmente protegidos

El capítulo IV de la ley establece en su artículo 18 que nadie estará obligado a proporcionar datos sensibles, entendiéndose por tales aquellos datos que revelen origen racial, étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o vida sexual, indicándose que sólo podrán ser tratados con el expreso consentimiento escrito del titular, y prohibiéndose la formación de bases de datos que almacenen información que directa o indirectamente revele datos sensibles.

Estos datos sólo podrán ser recolectados y tratados cuando medien razones de interés general autorizados por la ley, o cuando el organismo solicitante tenga mandato legal para hacerlo. También podrán ser tratados con finalidades científicas o estadísticas cuando los datos se disocien de sus titulares (cuando se elimine toda referencia que pudiera permitir relacionar los datos con su titular).

Quedan excluidos de la prohibición de la creación de bases de datos que almacenen estos datos sensibles las que posean los partidos políticos, sindicatos, iglesias, confesiones religiosas, asociaciones, fundaciones u otras entidades sin fines de lucro en cuanto a los datos de sus asociados o miembros. Sin perjuicio de ello, la recolección de esos datos precisará siempre la autorización previa del titular del dato.

Registro de las bases de datos de titularidad privada

La ley establece la obligación de la inscripción de todas aquellas bases de datos que no sean de uso exclusivamente individual o doméstico.

Como mínimo, y sujeto a lo que pudiera establecer la reglamentación de la ley, la inscripción deberá contener:

1) La identificación de la base de datos y el responsable de la misma.
2) La naturaleza de los datos personales que contiene.
3) El procedimiento de obtención y tratamiento de los datos.
4) Las medidas de seguridad y descripción técnica de la base de datos.
5) El destino de los datos y las personas físicas o jurídicas a las que pueden ser transmitidos.

6) El tiempo de conservación de los datos.
7) La forma y las condiciones de acceso a los datos de los titulares de los mismos, y los procedimientos para lograr su rectificación o actualización.
8) Datos relativos a la actividad crediticia de los individuos de acuerdo a lo establecido en el artículo 22 de la ley (tema que se tratará más adelante).

El artículo 29 de la ley también establece la prohibición a los usuarios de las bases de datos de poseer en las mismas datos personales distintos a los declarados en el registro.

Por último, se establece la prohibición a las empresas de servicios informatizados de datos personales que prestan servicios de tratamiento de datos a terceros, aplicar o utilizar los mismos con un fin distinto al que figure en el contrato de servicios o cederlos.

Organismo regulador

La ley 18.331 crea la Unidad Reguladora y de Control de Datos Personales encargada del control y aplicación de lo preceptuado.

Sus cometidos son:

- Asistir y asesorar a las personas acerca del alcance y contenido de la ley.
- Dictar las normas y reglamentaciones sobre la materia.
- Realizar un censo de las bases de datos alcanzadas por la ley y el registro permanente de las mismas.
- Controlar el cumplimiento de las normas sobre integridad, veracidad y seguridad de los datos.
- Solicitar información sobre el tratamiento de los datos personales a los usuarios de las mismas.
- Requerida, emitir opinión sobre las sanciones administrativas por el incumplimiento de lo establecido en la ley.
- Asesorar al Poder Ejecutivo en la redacción o consideración de proyectos de ley en la materia.
- Informar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de los responsables, en forma gratuita.

Sanciones

En caso de incumplimiento a lo establecido en la ley, la Unidad Reguladora podrá aplicar sanciones a los responsables de las bases de datos o a los encargados de su tratamiento.

Las mismas serán:

1) Apercibimiento
2) Multa de hasta quinientas mil unidades indexadas
3) Suspensión de la base de datos respectiva, pudiéndose promover ante los órganos jurisdiccionales correspondientes la suspensión de la base de datos hasta por un lapso de seis días.

Acción de Habeas Data

El artículo 37 de la ley declara el derecho de toda persona a entablar una acción judicial destinada a tomar conocimiento de los datos referidos a su persona, su finalidad y el uso que a los mismos se les da, que consten en bases de datos tanto públicas como privadas y, en caso de error o falsedad, discriminación o desactualización a exigir su rectificación o supresión o lo que se entienda pudiera corresponder.

Estudio particular de algunos puntos de especial relevancia

La comunicación de datos

Oportunamente se indicó que la comunicación de datos personales objeto de tratamiento sólo puede realizarse mediando el consentimiento expreso de su titular de los mismos el que será revocable. Se agrega ahora, que esos datos solamente podrán ser comunicados en cumplimiento de los fines legítimos tanto del emisor como del destinatario.

Sin perjuicio de la autorización que debe prestar el titular de los datos para que la comunicación de los mismos sea legítima, la misma no será necesaria cuando:

1) Así lo disponga una ley de interés general.
2) En el caso de las bases de datos excluidas de la obligación del previo consentimiento por parte del titular de los datos.
3) Se trate de datos personales relativos a la salud y su comunicación tenga por objeto estudios epidemiológicos, en casos de emergencias, o por razones de higiene o salud públicas. En estos casos la identidad de los titulares deberá preservarse mediante la aplicación de mecanismos de disociación de los datos.

4) En general, cuando se hubiera aplicado mecanismos de disociación de la información de modo tal que los titulares de los datos no puedan ser identificados.

El destinatario de esta información tendrá las mismas obligaciones legales y reglamentarias que el emisor de la misma y, muy importante, éste responderá solidaria y conjuntamente con el receptor por la observancia de las obligaciones que impone la ley, tanto frente al organismo de control como frente al titular de los datos. En otras palabras, si el destinatario de la información viola alguna de las obligaciones que la ley impone, el emisor de la misma será tan responsable como aquel.

Pero este tema tiene otra faceta y es la transferencia internacional de datos. Esta nueva ley prohíbe que la transferencia de datos personales se realice hacia países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo a los estándares internacionales salvo que:

a) el interesado haya dado su consentimiento inequívoco a la transferencia prevista.
b) La transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento.
c) La transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del titular del dato, entre el responsable del tratamiento y un tercero.
d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.
e) La transferencia sea necesaria para la salvaguardia del interés vital del interesado.

Sin embargo, prohibición no aplicará en determinados casos entre los que se cuentan los intercambios de datos de carácter médico cuando así lo exija el tratamiento del afectado por razones de salud o higiene pública, y las transferencias bancarias o bursátiles en lo relativo a las transacciones respectivas y conforme a la legislación que les resulte aplicable.

En definitiva, entendemos que este tema tiene particular importancia en casos de empresas sucursales de matrices en el extranjero cuando la sucursal debe remitir información. Pero particularmente delicado es la cuestión cuando la información

debe remitirse a, por ejemplo, servicios tercerizados de tratamiento de datos cuya locación se encuentre en países que pudieran no ofrecer las mismas garantías –o al menos similares- a las establecidas en nuestra legislación.

La protección de datos personales y el manejo de personal

El tema de la protección de datos personales es particularmente sensible en el área laboral y en lo que refiere a la contratación, evaluación y despido de personal.

En la etapa previa a la contratación de personal, esto es durante la evaluación, es importante informar al candidato que la información que proporcione (incluido su CV y la información de terceros) será evaluada por más de una persona o instituciones, y obtener su consentimiento escrito al respecto ya que podría existir la necesidad de corroborar con terceros la información proporcionada por el candidato.

El acto de decisión de contratar o no a un candidato –o de despedirlo- eventualmente puede tener como consecuencia una impugnación de esa decisión si la misma se tomó exclusivamente tomando en consideración los datos personales del candidato. Como se dijera, de acuerdo al artículo 16 de la ley, las decisiones que pudieran tener efectos jurídicos que afectaran de manera significativa a una persona y cuyo fundamento exclusivo fueran sus datos personales pueden ser impugnadas. Ahora bien, la ley no aclara cual será el mecanismo de impugnación de una decisión de carácter privado, o cual será la autoridad competente para decidir la misma, cuestiones que deberían ser resueltas por la reglamentación.

Otro punto a tener en cuenta durante el proceso de selección, es la obligación del empleador de deshacerse de la información del candidato que no fuera contratado una vez que la misma deja de ser necesaria para el fin para la cual fue recabada, o sea, una vez finalizado el proceso de selección. Esto podría eventualmente significar una afectación al derecho de defensa del empleador en caso de impugnación a la decisión de contratar o no al candidato de acuerdo a lo expresado en el párrafo anterior.

Durante la relación contractual, el empleado tendrá derecho a acceder a la información que el empleador tiene de él, y a solicitar su corrección o supresión en caso de error, exceso, falsedad, etc.

Por último, algunas reflexiones sobre el monitoreo de la actividad del empleado durante la actividad diaria en su lugar de trabajo. Sin perjuicio de no existir normas que específicas sobre la materia, existe una tendencia jurisprudencial en el sentido de otorgar al empleador el derecho a monitorear el uso que el empleado haga del correo institucional, el teléfono o el acceso a Internet. De todas maneras, es recomendable que en caso de instituirse estos controles se de aviso a los empleados en forma previa al comienzo de los mismos.

Conclusiones

La ley 18.331 no es del todo clara en muchos de sus conceptos. Más aun, en algunos es francamente vaga y lleva a confusión. La situación podría solucionarse una vez que el Poder Ejecutivo promulgue la reglamentación a la ley, cosa que hasta el momento no se ha hecho.

Hasta entonces, se deberá recurrir en forma permanente al organismo de control en busca de parámetros de acción en la aplicación de esta norma.

En virtud de lo anterior es que creemos conveniente realizar las siguientes recomendaciones a efectos de evitar al máximo la aplicación de sanciones por violación a lo establecido en la ley.

a) Revisar todos los procedimientos internos de recolección, tratamiento y comunicación de datos personales, tanto del personal de la empresa como de clientes.
b) Actualización de los formularios a efectos de que los titulares de los datos recabados otorguen los consentimientos que pudieran ser necesarios, informando además el fin que se dará a los mismos.
c) En caso de utilizarse bases de datos de terceros asegurarse del cumplimiento por parte de su responsable de la obligación de inscripción.
d) Mantener actualizadas las bases de datos y eliminar lo que no se utilice.
e) Implementar mecanismos de seguridad tendientes a asegurar la seguridad y confidencialidad de las bases de datos.
f) En caso de comunicación o transferencia de las bases de datos, confirmar los mecanismos de seguridad del receptor y la legislación vigente en el país de destino.
g) Inscripción de las bases de datos que se posean.