Fundación
Datos
Protegidos

Una propuesta a la ley de datos personales en Chile.

Los datos más allá de la privacidad

Datos Protegidos es una organización sin fines de lucro, que tiene como misión la promoción, defensa y fortalecimiento de los derechos de la privacidad y protección de datos. Promovemos discusiones en torno a la dignidad, igualdad y libertad de las personas en relación a la privacidad.

https://datosprotegidos.org/

La cuestión de los datos personales

El desarrollo tecnológico de las últimas décadas ha producido una de las transformaciones más revolucionarias de la historia de la humanidad. Todo aspecto de nuestra vida cotidiana ha estado directa o indirectamente influido por las nuevas capacidades de comunicación, almacenamiento y procesamiento de información, al igual que por los microchips e Internet, todo lo cual ofrece extraordinarias oportunidades para el desarrollo de la creatividad humana y, a la vez, importantes desafíos para el resguardo y promoción de derechos y libertades, tanto individuales como colectivas, en este nuevo ambiente digital.

En este contexto, de hiperacceso e hiperflujo de información, uno de los derechos que más se ha visto afectado es el de la protección a la relacionada a la vida privada de las personas, la cual está compuesta por una infinidad de datos que reflejan sus identidades, intereses, hábitos, relaciones humanas y movimientos diarios.

Los datos, de esa manera, han adquirido un valor inmensurable y se han convertido en el motor de la nueva economía dentro de la gran revolución digital. Hoy día quien tiene los datos, tiene el negocio, y muchas industrias se han dinamizado gracias al almacenamiento, procesamiento y transformación de datos personales. Este tratamiento masivo de los mismos ha estado en la base de muchas e importantes innovaciones, pero a la vez, ha expuesto, como nunca antes en la historia, la intimidad de las personas.

La tensión entre hiperaccesibilidad, tratamiento masivo de datos personales y la protección y resguardo de la esfera íntima de las personas, ha dado lugar a uno de los debates más relevantes en temas de derechos y nuevas tecnologías.

Este reporte busca plantear los puntos centrales del derecho a la protección de datos, identificando las principales falencias de la legislación chilena, revisando críticamente el proyecto de ley en tramitación y proponiendo aspectos claves que debiesen ser considerados en la discusión parlamentaria.

Para ello, se partirá de la base de la existencia de dos capas de control del derecho a la protección de datos personales: la primera capa, los derechos de las personas comúnmente conocidos como **ARCO**, por las iniciales de cada uno de estos derechos, acceso, rectificación, cancelación y oposición. La segunda capa es la existencia de las **autoridades u organismos de control en protección de datos**, que establecen los países para responder a los estándares internacionales en la materia. Lo determinante es que esta autoridad ejerza sus funciones con autonomía y que tenga atribuciones consultivas, de investigación, de intervención y sanción. El modelo europeo impulsa la creación de entes independientes e imparciales frente a los organismos públicos y privados y a personas que traten datos personales[1].

[1]Para más información puede consultarse Cerda Silva, A. (2006). Mecanismos de control en la protección de datos en Europa. Ius et Praxis, 12(2), 221-251.

Derechos ARCO

• **Derecho de acceso:** permite a los titulares de los datos personales acceder al registro o base de datos para conocer qué datos se tratan en ésta, cuál es su objetivo y quién los trata; cómo se obtuvieron, quién el responsable o controlador de dicho registro y si estos datos serán o no cedidos a un tercero.

• **Derecho a rectificación:** permite al titular de los datos corregir un dato incorrecto o desactualizado en un registro.

• **Derecho a cancelación de datos:** los datos contenidos en un sistema deben contar previamente con el consentimiento o habilitación legal de su titular y mantenerse en éste cuando exista una relación vigente con dicha persona. Este derecho obliga a eliminar estos datos si se pierde la habilitación legal para tratarlos; si se revoca el consentimiento por parte del titular, si hay un cambio en las circunstancias que dieron pie a su entrega o si hay modificaciones en los mismos.

• **Derecho de oposición:** es aquel que se ejerce en contra del responsable del registro, para impedir que se lleve a cabo el tratamiento de datos de carácter personal o bien frenar el mismo.

[¿De dónde surge el concepto?]

Fue en Alemania donde se sentaron las bases para configurar la garantía a la Protección de Datos Personales, mediante la consagración del derecho de toda persona a conocer y/o acceder a la información propia contenida en diversos ficheros públicos. Un primer hito es la Constitución de Weimar, la cual en 1919 permitió a los funcionarios públicos revisar su expediente personal dentro del aparato del Estado. Posteriormente, en 1970, el Estado de Hesse dictó la primera ley de protección contra el abuso de los datos, con ocasión del procesamiento en bases de datos electrónicas, tanto públicas como privadas, y sentó una serie de requisitos para la legalidad del tratamiento de datos. Siguen en esta línea las leyes de datos de Suecia en 1973, Francia, Austria, Dinamarca y Noruega en 1978, e Inglaterra en 1984[2].

Las primeras legislaciones de alcance e impacto internacional surgieron en 1981: la "Convención para la protección de los individuos en relación con el procesamiento automatizado de datos", Convenio 108 del Consejo de Europa[3], y las "Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales" de la Organización para la Cooperación y el Desarrollo Económico (OCDE). Los tres documentos contienen los principios de protección de datos vigentes hasta hoy, la libertad y la privacidad de las personas, que están en el "corazón" de este derecho.[4]. **El objetivo principal de estos acuerdos es económico, pues se orientan a solucionar disparidades en las legislaciones nacionales, eliminando obstáculos para la libre circulación de los datos a nivel transfronterizo.**

[2]Muñoz de Alba Medrano, Marcia. Habeas Data. [En línea] <http://biblio.juridicas.unam.mx/libros/5/2264/4.pdf> [Consulta agosto 2017]
[3]Convenio 108 de 1981. En línea [http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm]
[4]Heredero, Manuel. (1997) La directiva comunitaria de Protección de datos de carácter personal. Editorial Aranzadi S.A.

A partir de este punto, se produce una evolución del derecho a la protección de datos personales, pasando desde una faz económica hacia una concepción global que involucra los derechos humanos. Así, se buscó conciliar el propósito económico y social de la libre circulación de los datos, con el resguardo a la privacidad y la autonomía de las personas.

En la construcción de este derecho se plasmaron "dos libertades personales": la autodeterminación informativa y la libertad informática. La primera es la facultad de la persona para decidir por sí misma cuándo y dentro de qué límites revelará situaciones referentes a su propia vida. La segunda es la "autotutela" de la identidad, es decir, el derecho a controlar los datos personales frente a su tratamiento automatizado o manual dentro de un sistema informático o una base de datos[5]. Esto puede llevarse a cabo a través de la ley o mediante la intervención de la autoridad que vela por la protección de datos de las personas.

[5]Duran, Lucas. (1997) El acceso a los datos en poder de la administración tributaria.

[Los datos personales en Chile]

En nuestro país la protección de datos se ha vinculado con el derecho a intimidad, en el artículo 19 de la Constitución, el que asegura a todas las personas **el respeto y protección a la vida privada y a la honra de la persona y su familia**. El año 2010 un fallo del Tribunal Constitucional reconoció, por primera vez y expresamente, "la estrecha relación entre la vida privada de las personas y la protección de sus datos personales, bajo lo que la doctrina denomina autodeterminación informativa"[6]. Así, se expresa la "relación de pertenencia entre ambos derechos", anclando constitucionalmente la protección de los datos a la protección de la intimidad.

Así todo, el efecto de la protección de datos no puede acotarse solo al resguardo de la intimidad. Un tratamiento ilegítimo de éstos puede además afectar otras garantías, como el acceso al empleo, a la educación o a la salud, en cuanto la protección no es sólo confidencialidad, sino la creación de un entorno de condiciones para el pleno ejercicio de derechos vinculados a la personalidad y dignidad de las personas, en un contexto digital en que casi toda nuestra identidad se reduce a datos.

El último gobierno de Michelle Bachelet presentó –en marzo de 2017- un proyecto de ley que regula la Protección y el Tratamiento de los Datos Personales y crea la Agencia de Protección de Datos Personales (Boletín N°11.144-07), el que se refunde con una iniciativa parlamentaria, presentada en enero de 2017, que va en la misma línea proteccionista.

[6]Requerimiento de inaplicabilidad por inconstitucionalidad. ROL 1732- 10 INA y ROL 1800-10 INA. Acumulados. Jorge Cabezas Villalobos y otros trabajadores de Televisión Nacional de Chile respecto del artículo décimo, letra h), de la Ley N° 20.285.
En línea [http://www.tribunalconstitucional.cl/wp/descargar_sentencia.php?id=198

Esta iniciativa legal viene a cubrir una profunda deuda respecto al cumplimiento de los estándares internacionales en la materia. Desde la irrupción de internet a la fecha, los ciudadanos chilenos solo cuentan con la Ley de Protección a la Vida Privada (Ley N° 19.628), que data de 1999, y que ha recibido reiteradas críticas desde organizaciones de la sociedad civil y expertos por su débil protección a los datos personales. En Europa, se ha tomado nota de esta legislación extemporánea, lo que ha afectado el desarrollo de actividades económicas vinculadas a transferencias internacionales de datos. En la misma línea, la Organización para la Cooperación y el Desarrollo Económico (OCDE), se ha manifestado frente a ello instando a que se fortalezca la legislación interna.

Ley de Protección a la Vida Privada: una mirada blanda a los datos personales

La ley 19.628, de fines de los noventa, es la primera de su tipo en América Latina. Contiene una serie de definiciones relevantes, fija requisitos para el tratamiento de datos personales, norma el actuar de los responsables de bases de datos y reconoce, por primera vez, los derechos de los titulares de datos (derechos ARCO) en la legislación chilena. Acoge el principio de finalidad en el tratamiento de datos y fija normas para la utilización de datos personales frente a obligaciones de carácter bancario o comercial y el tratamiento de datos por organismos públicos.

Desde su dictación esta ley ha sido objeto de reiteradas y variadas críticas, por conceptos incompletos, dificultad y costo para ejercer derechos y por la ausencia de una autoridad de protección de datos que vele por el cumplimiento de la ley, , lo que ha traído consigo que esta ley sea desconocida y poco ejercida en los casi 20 años de vigencia.

La ley actual establece lo que debe entenderse por datos personales, datos sensibles, datos caducos y lo que es un banco de datos, definiciones que resultan positivas para entender la normativa, pero requieren de una actualización.

En particular, preocupa la amplia definición de **fuente de datos accesibles al público**, que en la práctica significa que todos los datos de fuentes de acceso público pueden tratarse libremente, no siendo necesario el consentimiento de las personas dueñas

de los datos. La fuente de acceso público, no se define, debido a una transcripción incompleta de la norma en la que se inspiró la ley chilena y en la práctica, quien crea la base de datos, define si se trata de una base de datos de acceso público o no. **También se observa un vacío en la definición de los distintos actores que participan del tratamiento de datos (controlador, encargado, intermediario), como la indicación de sus deberes y obligaciones, cuyo incumplimiento debe acarrerar una sanción.**

En el mismo sentido, la estructura de los principios consagrados en esta ley no entrega suficientes garantías para alcanzar un equilibrio entre la libertad para tratar datos personales y el derecho a la privacidad e intimidad de las personas. La **amplitud de las excepciones** a la necesidad de obtener el consentimiento por parte del titular, merma su efectividad como resguardo. Y falta, entre muchas otras, una referencia especial a los menores de edad, que son especialmente vulnerables.

En consecuencia, el problema fundamental de la ley es que su prioridad u objeto no está en proteger a los individuos del tratamiento de sus datos realizado por terceros, sino en regular al mercado del tratamiento de datos personales, lo que se refleja en la ausencia de sanciones efectivas ante la vulneración de las normas; la falta de regulación para el flujo internacional de los datos personales; el uso de datos personales para marketing directo sin autorización del titular y la inexistencia un registro de bases de datos privadas, entre otras.

Para ejercer el derecho al control de los datos, los recursos que ofrece la ley son totalmente deficientes e insuficientes. La falta de una autoridad que pueda asegurar el cumplimiento de las obligaciones contenidas en la ley, es su gran vacío. Contar con esta autoridad permitiría a los titulares y a los responsables

de datos llevar a cabo procedimientos más expeditos sin intervención de la justicia en una primera instancia. Lo anterior, también contribuiría a desarrollar procedimientos para la prevención de eventuales infracciones, como la disminución de los daños posteriores.

Una reforma en lista de espera

Las deficiencias y limitaciones de la actual ley de protección de datos personales (Ley Protección a la Vida Privada) exigen con urgencia una actualización que permita regular el **tratamiento y la transferencia de datos personales, superponiendo y privilegiando la protección y defensa de los derechos de las personas.** Cabe tener presente que esta normativa fue elaborada en una época en que el desarrollo y el acceso a las tecnologías y redes era escaso y que, por el contrario, hoy existen capacidades de almacenamiento ilimitado, de tratamiento automatizado de datos y facilidades para el flujo de éstos fuera de las fronteras de los países.

> El eje principal de una reforma legal debe estar en estructurar un conjunto de derechos y principios que resguarden adecuadamente a las personas ante los riesgos del tratamiento automatizado de datos y crear una Agencia de Protección de Datos que garantice el resguardo de dichos derechos, adecuándose al estándar internacional.

Respecto a estos derechos y principios de los ciudadanos, es imperativo restringir los casos de excepción al consentimiento y adoptar los principios reconocidos por la OCDE, tales como proporcionalidad, calidad de los datos, especificación del propósito o finalidad, limitación de uso, temporalidad, seguridad de los datos, acceso y oposición de su titular, y transparencia, entre otros. En cuanto a un organismo regulador, éste debe ejercer sus funciones con total independencia y contar con atribuciones consultivas, investigativas, interventivas y de sanción.

Revisión al proyecto de ley del Gobierno de Chile

La Presidenta Michelle Bachelet presentó en marzo de 2017 un proyecto de ley de Protección y Tratamiento de Datos Personales el cual propone la creación de una Agencia de Protección de Datos Personales. Proponemos un conjunto de mejoras en base a la **protección de derechos, autoridad, autorregulación, órganos públicos, transferencias internacionales de datos y foco territorial.**

Ajustes necesarios al proyecto de ley

El corazón de una ley de protección de datos personales está en los principios y definiciones que permiten determinar los roles, derechos y deberes de los actores que participan en el tratamiento de la información de las personas. Su estructura debe ser suficientemente flexible para adaptarse a la constante evolución de las tecnologías y clara y precisa en identificar en qué es lo que debe ser protegido.

Es posible encontrar referentes internacionales con definiciones y criterios de aplicación mejor construidos para asegurar la protección de los derechos de las personas. Del análisis de la ley actual, los proyectos y dichos referentes, **recomendamos:**

– El objeto de esta ley debe, ante todo, asegurar el respeto de los derechos y libertades de los titulares de datos, mediante el control de los mismos y su adecuado tratamiento, y no al revés, como señala el proyecto de ley y la normativa vigente.

– La ley de datos debe ser general y aplicarse de manera supletoria a otros tratamientos regulados por leyes especiales. Ejemplo: datos en salud, telecomunicaciones, tránsito, etc.

– **La** definición de datos sensibles debe ser amplia y no cerrada a determinada categoría de datos, dado que un dato puede llegar a ser personal sensible si su tratamiento da origen a una discriminación arbitraria o ilegal o conlleve un grave riesgo para su titular.

– El concepto de fuentes de acceso público se ha prestado para abusos debido a su ambigüedad, por lo cual se esperaría que estas fuentes fueran específicamente o precisamente definidas Por ejemplo, una base de datos o datos que se publican en Internet quedan desprotegidos y existe el riesgo de que un privado los utilice desvirtuando la finalidad para la cual fueron entregados y sin autorización del titular.

– El principio de proporcionalidad debe perfeccionarse con una "minización de datos", es decir establecer que se soliciten solo los datos pertinentes al objetivo que se busca, reduciendo así su recolección al mínimo.

– Se debe contemplar el principio de temporalidad, el cual significa que el tratamiento de los datos no puede ser indefinido en el tiempo.

– El principio de calidad significa que los datos deben ser exactos, actuales, veraces y el responsable de las base de datos debe entregar las herramientas a los titulares para que estos puedas actualizarlos cuando sea necesario.

-Principio de responsabilidad. Debe imponerse al responsable del tratamiento de los datos el deber de comprobar que ha cumplido con las obligaciones legales y no al revés. Laprueba sobre el mal o buen tratamiento de datos no debe recaer en el titular.

– Principio de seguridad. El tratamiento de datos personales debe garantizar niveles adecuados de confidencialidad, integridad y disponibilidad, y declararse esto expresamente en la ley. La figura de "daño accidental", diezma el sentido del principio. La mayoría de las leyes contemplarán un nivel

de protección sobre los datos que se condiga con el riesgo, y el riesgo dependerá del contexto.

– El derecho a rectificación ordena que la modificación de los datos y su contenido serán públicos, lo que es problemático puesto que los datos personales no son públicos en algunos contextos.

– El deber de secreto o confidencialidad debe mantenerse aún después de cesar las actividades de tratamiento por parte del responsable o sus dependientes de manera indefinida.

– En cuanto al deber de reportar las vulneraciones a las medidas de seguridad que pesa sobre los responsables, el proyecto debiera contemplar que esta notificación a los titulares se lleve a cabo siempre que exista un riesgo y no acotarlo a la vulneración de un dato sensible.

– Datos personales relativos a la salud. Una de las excepciones que contempla el proyecto para requerir el consentimiento por parte del titular de los datos, tiene lugar "cuando resulte indispensable para la ejecución o cumplimiento de un contrato cuyo objeto o finalidad exija tratar datos relativos a la salud del titular." La norma debe referirse específicamente al tratamiento en el marco de una prestación de salud y no en los contratos cuyo objeto exija tratar datos de salud por su finalidad. Lo anterior puede dar lugar, por ejemplo, a que un contrato bancario exija el tratamiento de datos de salud, en circunstancias que la finalidad del contrato bancario es distinta.

Qué no puede faltar:

1. Reconocimiento de nuevos derechos

1.1. Derecho a la Portabilidad.

Las personas debieran tener el derecho a recibir, en un formato estructurado, de uso común y lectura mecánica, todos los datos referidos a su persona cuando hayan sido entregados previamente a un registro para su tratamiento, en un ejercicio equivalente al llevado a cabo en la portabilidad numérica de telecomunicaciones.
Esta entrega de datos debe ser sin impedimento alguno y debe tener lugar cuando, entre otros casos, se haya terminado la relación contractual con la empresa, la cual no podrá mantener copia nominativa alguna. Este derecho deberá implementarse de manera adecuada por las empresas debiendo evaluar diversos tipos de datos y sectores, salud, educación, etc.

1.2. Posibilidad de impugnar o reclamar frente a las decisiones automáticas (Impugnación valoraciones personales).

Quienes tratan datos no podrán adoptar decisiones que se basen únicamente en valoración, evaluación o predicción del comportamiento realizada con tratamiento automático de datos personales. Es decir, las personas deben tener derecho a impugnar la utilización de sus datos personales para evaluar determinados aspectos de su personalidad, como su rendimiento laboral, hábitos, conducta e historial crediticio, cuando éstas se tomen solo usando medios mecánicos y no exista intervención humana.

2. Ampliación de concepto de dato personal

La aparición de nuevas tecnologías ha ampliado las formas de obtención de datos personales y de generación de información que permite identificar a una persona. Por ello una reforma a la ley debe contemplar un concepto amplio de dato personal que posibilite contener todos aquellos elementos identificables de un individuo.

Videovigilancia. La captación y/o el tratamiento de imágenes con fines de vigilancia se ha establecido como norma en la mayoría de las grandes ciudades del mundo. Los datos procedentes de imágenes y sonidos de videocámaras son datos personales pues se refieren a personas identificadas o identificables y, por tanto,deben regirse por esta legislación como base.

Otro ámbito de datos que debe incorporarse es la **información de la geolocalización**. Estas herramientas, presentes en aplicaciones móviles, en la medida que pueden recoger patrones de comportamiento de las personas, son datos que permiten identificar a un individuo y, por tanto, se consideran datos personales.

Lo mismo ocurre con todos los **metadatos de las comunicaciones de las personas**. Los metadatos son los llamados “datos de los datos”, se trata de los registros como el horario, tráfico e información sobre quien emite y recibe la comunicación. En estos metadatos también se encuentran datos personales, cuando de los patrones de comportamiento se puede extraer la identidad de la persona, por ende, deben regirse explícitamente por esta ley.
Los datos de niños y niñas, merecen mención especial en la ley y especial protección.

3. Autoridad de Protección de Datos

Lo más importante en este punto es independencia de la autoridad de control. Esto se logra con estableciendo condiciones especiales en relación **al nombramiento** de la autoridad, para que ésta sólo pueda ser removida y sancionada por causales concretas y para que permanezca en su cargo inamovible por un periodo fijo. El gobierno de turno no debe ser capaz de ponerle fin, debe existir la posibilidad de renovación y no coincidir con periodos de cambio de gobierno. Las causales de **remoción** deben estar expresamente establecidas en la ley y exigirse adicionalmente determinadas condiciones.

El requisito de **independencia** no se cumple cuando el responsable de la autoridad es un funcionario del Estado sometido a supervisión jerárquica; la autoridad de datos debe ejercer sus funciones sin influencia externa. Esto implicaría toda orden directa o indirecta que pudiera orientar sus decisiones y, en consecuencia, poner en peligro el cumplimiento de la tarea de las autoridades establecer un justo equilibrio entre la protección del derecho a la intimidad y la libre circulación de datos personales. El director de la autoridad no debe ocupar simultáneamente otras posiciones gubernamentales. Por último, debe disponer de una línea presupuestaria autónoma para asignar los medios humanos y materiales.

La autoridad debe, asimismo, tener la facultad de **fiscalizar** las operaciones de tratamiento de datos personales; de requerir información de quienes tratan datos y resolver los reclamos que formulen los titulares de datos por infracciones a la ley. También le corresponde **sancionar**, en primera instancia, a quienes infrinjan la ley de datos, salvo respecto de los órganos públicos, que deberá ser resuelto por tribunales. Por último, le corresponde **interpretar** administrativamente las disposiciones legales en

materia de protección y tratamiento de datos personales, dictar normas generales e impartir instrucciones para su aplicación y fiscalización.

Para lo anterior, debe reconocérsele un procedimiento y capacidad para realizar inspecciones y visitar los establecimientos, teniendo los responsables que dar las facilidades para que la autoridad pueda cumplir sus funciones. Los hechos constatados por los inspectores de protección de datos, que informan de oficio o a requerimiento, deben constituir presunción legal de veracidad para todos los efectos legales, incluso para los efectos de la prueba judicial. Del mismo modo, si las circunstancias lo ameritan, deben tener la posibilidad de solicitar el auxilio de la fuerza pública, actuar de oficio, ordenar la suspensión inmediata de las labores que, a su juicio, constituyan infracción a la ley, y levantar una multa.

Debe tener conocimiento de las infracciones hacia los organismos públicos y dictar instrucciones, fiscalizar y emitir dictámenes obligatorios para éstos. Asimismo, sus competencias deben ser exclusivas y no compartidas con otros entes públicos.

4. Modelos de autorregulación

La Red Iberoamericana de Protección de Datos, desde el año 2004, reconoce e impulsa la promoción de iniciativas de autorregulación sectorial, que complementen y faciliten la aplicación de las leyes de protección de datos. La autorregulación se compone de **instrumentos precisos para potenciar el tratamiento adecuado de éstos**, complementando o desarrollando los marcos regulatorios existentes, siempre aprobados por una autoridad de control. Agregan así un valor de garantía, calidad y confianza, sin perjuicio de las obligaciones establecidas en la normatividad vigente en materia de protección de datos.

5. Regulación ante organismos públicos

La conciliación del acceso a la información pública y la protección de datos es fundamental. Debe superarse la errada idea de que se trata de dos caras de una misma moneda. La información de una persona no se transforma en información pública por el solo hecho de encontrarse en poder de un organismo público, al contrario, éste debe aplicar la correspondiente causal de reserva basado denle la protección del derecho a la privacidad de las personas.

Por otra parte, las posibles solicitudes a través de la Ley de Acceso a la Información solo podrán recaer sobre los métodos de tratamiento de los datos, las formas de recopilación o uso de éstos y no sobre los mismos. Esto a menos que se trate de los datos propios del solicitante.

Cuando la ley decida excluir al Estado de la aplicación de la ley de datos, debe hacerlo por motivos fundados. No corresponde señalar, por ejemplo, que no se aplican ninguna de las disposiciones de la ley en ciertas actividades estatales como la seguridad pública. Cosa distinta es que se limite el ejercicio de derechos ARCO, en actividades del Estado, específicamente cancelación y oposición.

El Estado siempre deberá respetar al menos los principios de datos personales.
Casos en que exista tratamiento de datos personales en telecomunicaciones, seguridad pública o vigilancia deben ser regulados y la agencia debe tener las facultades de verificar la legalidad y proporcionalidad de estas acciones.

6. Transferencias internacionales de datos

Un tipo de tratamiento de datos tiene lugar en su transferencia internacional, es decir, cuando existe un movimiento de los datos más allá de las fronteras nacionales para su procesamiento, almacenamiento o recuperación. Respecto a ello, los principios básicos que regulan la protección de los datos personales a nivel nacional deben aplicarse a nivel internacional.
El objetivo de contar con normas en materia de movimientos transfronterizos de datos y una ley acorde a los estándares internacionales, es la posibilidad de contar con la **declaración de "país adecuado" en materia de datos frente a Europa**, como lo son Argentina, Uruguay y Colombia, próximamente. Como esto no ocurre en la actualidad, para que se pueda autorizar una transferencia de datos desde la Unión Europea a nuestro país, no basta con que las empresas responsables chilenas ofrezcan garantías suficientes de protección de la vida privada de las personas, las que pueden derivar de cláusulas contractuales, sino que también se requiere autorización de la autoridad de datos del país exportador. En razón de ello,el número de contratos internacionales ha disminuido considerablemente en los últimos años.

7. Aplicación territorial

La ley debe definir un ámbito de aplicación territorial. **La protección de los datos es un derecho escudo en la era digital y un derecho habilitador para la protección de otros derechos fundamentales. La sobreexposición de información ha generado que otras garantías se vinculen a la protección de datos, como el honor y la rehabilitación o el perdón a las personas mediante la institución de la cancelación de datos, hoy conocido como "derecho al olvido", lo que no es algo nuevo.**

El **"derecho al olvido"** comúnmente se pone en disputa con el derecho de acceso a la información y libertad de expresión y también entra en conflicto la territorialidad de la aplicación de soluciones jurídicas. Esto dice relación con la esfera de aplicación de la ley, si debe ser local o global para que sean eficaz. La respuesta parece ser fácil: una sentencia se aplica dentro de las fronteras nacionales en las que opera una autoridad legal; sin embargo, en Internet el espacio está hecho de datos, URL, códigos, protocolos.

Una sentencia que se aplica a Internet no puede depender entonces de la solución territorial, puesto que Internet no es un territorio. Este pilar del derecho clásico queda totalmente desvirtuado y desfasado.

¿Quien manda en Internet? Para las personas comunes y corrientes, la ley de internet son las condiciones de uso que imponen las grandes empresas: Google, Twitter, Instagram, Whatsapp y otros dominadores de la red, las que son iguales para todos Se hace entonces necesaria la creación de herramientas para las personas que permitan que las decisiones de un Estado que busquen proteger derechos sean eficaces en Internet.

Fundación
Datos
Protegidos