Clase 4: Protección de datos personales.

Diplomado de Ciencia de Datos

Notas por José Daniel Conejeros - jdconejeros@uc.cl

Junio del 2020

Profesor: Victor Andrade - contacto@victorandrade.cl

I. Descripción del escenario actual

En la actualidad Chile si cuenta con una ley de protección de datos personales que está disponible desde el año 1999. Luego de 3 años de tramitación aparece la ley Nº19628 de Protección de Datos Personales (**LPD**), no obstante, una de las complicaciones es que en 1999 el nivel de interacción con internet era bastante bajo, en otras palabras la generación de data era limitada, lo que se distancia con los grandes volúmenes de información que se generan en la actualidad.

A pesar de que la ley existe, esta no es apropiada ya que no provee lo mínimo para una normativa de datos personales:

1. Un adecuado estatuto para la protección de los titulares de los datos personales.
2. Dar un marco para el mercado de la información respetando el derecho de las personas.

En primer lugar, esto ocurre ya que es una ley que requiere actualizaciones constantes pues el contexto tecnológico sigue cambiando y ampliandose. De hecho, lo que antes no era considerado un dato personal hoy puede serlo dado su potencial de identificar a las personas. En esa línea, **un marco de regulación debe ser capaz de actualizarse a sí misma para dar respuesta independiente el marco tecnológico en el que estemos**.

En segundo lugar, **no hay una agencia o institución a cargo de hacer cumplir la ley**. No hay una agencia de protección de datos y dado que no tenemos una autoridad hay cosas que no se deben hacer, pero que se hacen de todas maneras. La carencia de una institución ha invitado a la participación de otros actores a través de sus propias leyes y nichos, lo que ha llevado a desarrollos independientes sobre estos temas. En definitiva, cada institución tiene su propia interpretación respecto a la protección de datos personales y **no se contempla una institucionalidad común**. Ejemplos son la intervención del SERNAC, el sistemas de salud y derechos del paciente o el Consejo para la Transparencia en organismos públicos.

Diagnóstico Inicial:

- No tenemos agencia para la protección de datos personales.
- Hace poco tiempo (2018) se modifico la constitución incorporando el derecho a la protección de datos personales.
- Hay dos proyectos que buscan reformar y modernizar la ley de 1999 para equipararla a lo que existe en otros paises.

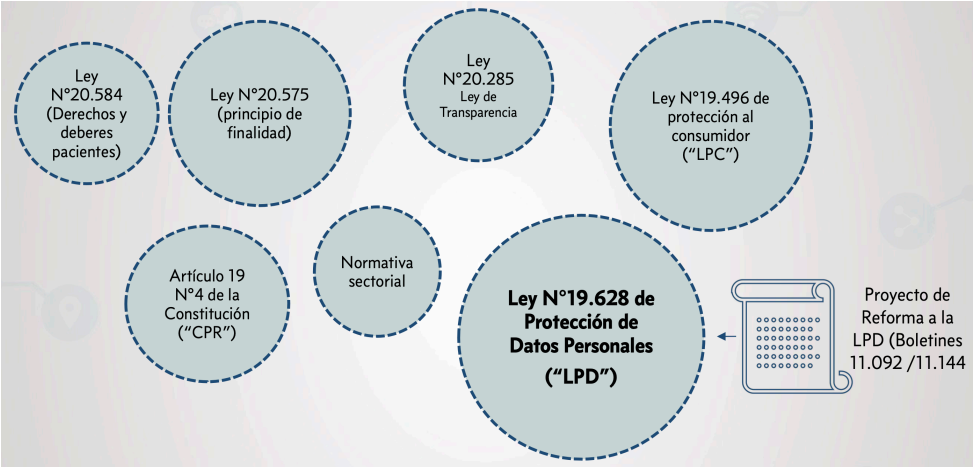

Figura 1: Normativa vinculada a la protección de datos personales

¿Qué ha llevado a la fragmentación del sistema?

a. Reguladores que han interpretado y aplicado la LPD

Cada una de las autoridades ha aplicado visiones propias sobre la protección de datos personales:

- Superintendencia de pensiones: datos para pensionados.
- Servicio de Impuestos Internos: datos para personales naturales (EIRL).
- Superintendencia de electricidad y combustibles: datos de consumo electrico.
- Comisión para el mercado financiero: deudas de los individuos que es manejado por los bancos.
- Consejo para la transparencia.

En definitiva hay múltiples actores que abordan el tema pero no es un trabajo coordinado. Recién aparecería una coordinación regulatoria en el proyecto de reforma de la LPD incluyendo últimas indicaciones que ortogaría al Consejo para la Transparencia (CPLT) el rol de autoridad de control de datos personales, pasando a ser el **Consejo para la transparencia y la protección de Datos Personales**. Cada vez que otro actor quiera realizar una acción/decisión sobre datos personales debe ser gestionado a través de este actor central.

b. Conflictos sobre aplicación de la LPD

- Fallos de la Corte Suprema sobre acciones de protección que se han referido sobre la aplicación de la LPD a personas jurídicas en lo que respecta a publicación de deudas y morosidades en registros de burós de crédito (Ej: Dicom - Equifax).
- Grado de especialidad de normas sobre secreto y reserva de determinada información respecto de la LPD (Ej: información manejada por la CMF sobre deudas en sistema bancario).
- Rol del Consejo para la transparencia y la protección de Datos Personales y ponderación entre transparencia y protección de datos. Conflicto de interés no menor, por lo que se deberían disociar las decisiones.

Es por esto que el tema se ha ido trabajando cada caso.

c. El proyecto de Ley

Reforma constitucional (Ley Nº21096) se agrega el derecho a la protección de datos personales. Artículo 19:

> La constitución asegura a todas las personas: (4) El respeto y protección a la vida privada y a la honra de las personas y sus familias, y asimismo, **la protección de sus datos personales**. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley.

Antes de esta modificación en 2018 si había una protección de datos personales, pero se entendía que los datos personales eran solo una extensión a la vida privada. Sin embargo, la experiencia va dando cuenta que no es así para todos los casos, por ejemplo, con el asunto del DICOM que maneja bases de datos de morosidad. En un principio estaba justificado la existencia de información pública sobre el riesgo de prestar dinero a una persona para el bien común, pero esto comenzo afectar otros derechos personales como la educación, salud, trabajo, etc. No en todos los casos el uso de datos personales lleva a afectar la intimidad (la privacidad) de otra persona, sino que el uso de esta información puede generar discriminación hacia el acceso de otros derechos. Que en los derechos personales esté en la constitución es importante porque si en algún momento hay un conflicto de transferencia de información y seguridad pública, habrá quienes busquen ponderar los derechos de la datos personales.

En línea con lo anterior, se genero un proyecto de reforma integral a la LPD que busca modernizar el sistema.

- Refunde el mensaje del ejecutivo y la moción parlamentaria.
- Actualmente se encuentra en primer trámite constitucional en el Senado.
- El 6 de julio de 2018 se presentó el último paquete de indicaciones.

Dado los compromisos asumidos por el país a nivel internacional, es un proyecto que tiene un cierto nivel de apuro para que quede en vigencia con las especificaciones requeridas en el menor tiempo posible.

II. Conceptos Claves

Respecto a las definiciones claves de la ley vigente, a su vez, la mayoría de las legislaciones a nivel global utilizan conceptos similares:

a. Titulares de datos: la persona natural a la que se refieren los datos de carácter personal. Las personas jurídicas no son titulares de datos de caracter personales, las empresas no son titulares de datos. El titular del dato refiere a que pueden gestionar los datos según estimen conveniente (dentro de ciertos margenes), no son derechos de propiedad, sino que de gestión.

b. Datos personales: los relativos a cualquier información concerniente a personas naturales (porque los titulares son), identificadas o identificables (esto nos permite saber si con la data es suficiente para llegar a la persona). Ejemplos: El rut es un dato personal pues permite identificar a alguien, si le quito el dígito de verificador sigue siendo un dato personal pues es la suma de todos los datos. El número telefónico es un dato personal, pues permite identificar a alguien, pero no autentica a una persona. El **identificable** es un dato con potencial de identificación una vez tratado, en este caso, podrían ser la IP, ya que es un dato que permite identificar a un individuo acotando a un numero reducido de las personas. Lo más relevante es **disociar la identificación con la autenticación**, los datos sirven para identificar, pero no necesariamente autentificar. Se agregan los datos de on-line como dato personal, identificador de una cuenta on-line. Si utilizo un dato con fines específicos y ese dato permite identificar a un individuo estoy en el campo de los datos personales. Los identificadores ficticios pueden ser personales mientras se puedan acceder a la información de los individuos (información pseudoanimizada, ejemplo el mrun que utiliza el mineduc por una razón de seguridad). Otro ejemplo, es el uso de la tarjeta bip como potencial identificable.

c. Datos sensibles: aquellos datos personales que se refieren a las características físicas o morales de las

personas o a hecho o circunstancias de su vida privada o intimidad, tales como los hábitos personales, etnia, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual. Los datos sensibles son datos personalkes, pero es una categoría de mayor importancia. Por ejemplo los antecedentes penales que tienen una calificación negativa de las personas (son propios de nuestra intimidad). No implica que no se puedan tocar, sino que requiere un tratamiento personal. Todas las personas tratan datos sensibles, por ejemplo, en recursos humanos que tratan licencias médicas que entrega información de un trabajador. Por ejemplo, en la ciencia de datos, el análisis de sentimiento y el análisis de texto utiliza información sensible pues revela ideas, posiciones políticas, morales, identidad de género, etc. En empresas es el uso de esa información para aplicaciones comerciales. Eliminar los hábitos personales puede ser un defecto pues todo puede ser un hábito personal, eso puede llevar a que todo sea tratado como dato personal, lo cual es una desfiguración de la ley.

d. Tratamiento de datos: cualquier operación o complejo de operaciones o procedimientos técnicos de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal o utilizarlos en cualquier otra forma. No queda fuera ninguna operación relacionada al ciclo de vida del dato (desde que se recolecta hasta que se elimina). Se debe buscar que el tratamiento esté dentro de un marco legal, no buscar si hay algún actividad que esté fuera de esta categorización.

e. Dato estadístico: el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable. Concepto de ley, pero no es recomendable de usar, pues lo más apropiado es usar datos anonimos y/o disociados. El dato que nunca fue dato personal o el dato que al principio era dato personal, pero con un tratamiento dejo de ser dato personal. Por ejemplo, la agregación y desagregación de los datos. Hay criterios internacionales para anonimizar datos, es importante saber cuándo vamos a trabajar con datos anonimizados. Encriptar los datos será una pseudoanonimización y es un tratamiento de datos. No es per se ilícito trabajar con datos no anonimizados, va a depender del tratamiento (uno puede solicitar autorización).

f. Responsable del tratamiento: persona natural o jurídica privada o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de caracter personal. En el caso de que el tratamiento de datos personales se efectúe por mandato se aplicará las reglas generales. El responsable es el que toma decisiones respecto al tratamiento, el mandatario de procesamiento mientras siga las instrucciones delega al responsable del tratamiento toda la responsabilidad de que el manejo de datos de personales sea lícito.

Algunos ejemmplos:

- Dirección IP: dato personal identificable de una persona.
- Medidores inteligentes: Información de los hábitos de personas que viven en un hogar. Se puede obtener mucha información a través de estos medidores.
- Datos encriptados: es una medida de seguridad.

III. Fuentes de tratamiento

a. Licitud del tratamiento de datos

> Artículo 4º.- El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.

Regla general: Consentimiento del titular de datos. Debe ser expreso (yo consiento), informado y constar por escrito. No necesita ser firmado en papel dado que 1. puede estar en marco en un archivo electrónico y en 2. debe tener la autenticación (la persona que está haciendo un acto es quien dice ser). El titular tiene el derecho de revocar sin efecto retroactivo su consentimiento, aunque hay tratamiento que son conaturales al servicio.

b. Excepciones al consentimiento:

1. Datos que se recolecten de fuentes de acceso al público cuando (no se requiere consentimiento):

- Se trate de datos de carácter económico, financiero, bancario o comercial.
- Se encuentre contenidos en listados que indiquen la pertenencia de la persona a una categoría tal como profesión o actividad, títulos educativos, dirección o fecha de nacimiento.
- Sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

2. No se requerirá autorización cuando el tratamiento de datos personales sea realizado por entidades privadas para su uso interno (incluyendo sus miembros y otras entidades afiliadas) para fines de tarificación, estadísticas o similares (sin referencia a una persona en particular).

c. Datos Sensibles

> Artículo 10º.- No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

IV. Derechos del titular de datos (artículos 12 y 13)

- Derecho de acceso a información
- Derecho de rectificación, cancelación y bloqueo
- Derecho de copia

> El responsable debe pronunciarse sobre la solicitud del titular en el plazo de dos días hábiles, salvo que deniegue la petición por motivos de seguridad de la Nación o interés nacioanl.

V. Obligaciones del Responsable de Datos

> Artículo 11º.- El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.
>
> Artículo 23º. La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.

VI. Proyecto de Ley I

Figura 2: Proyecto de Ley

a. Regla general (artículos 12 y 13 del proyecto):

Consentimiento libre, informado, específico, manifestado de manera inequívoca, **mediante declaración verbal**, escrita, **medio electrónico o acto afirmativo que de cuenta con claridad la voluntad del titular**

b. Otros fundamentos

Se mantienen los casos de fuentes de acceso público y lo relativo a datos económicos y se agregan:

- Datos necesarios para ejecución cumplimiento obligación legal.
- Datos necesarios para ejecución contrato o medidas precontractuales.
- Satisfacción de "intereses legítimos" del responsable.
- Datos necesarios para el ejercicio de derechos ante tribunales.

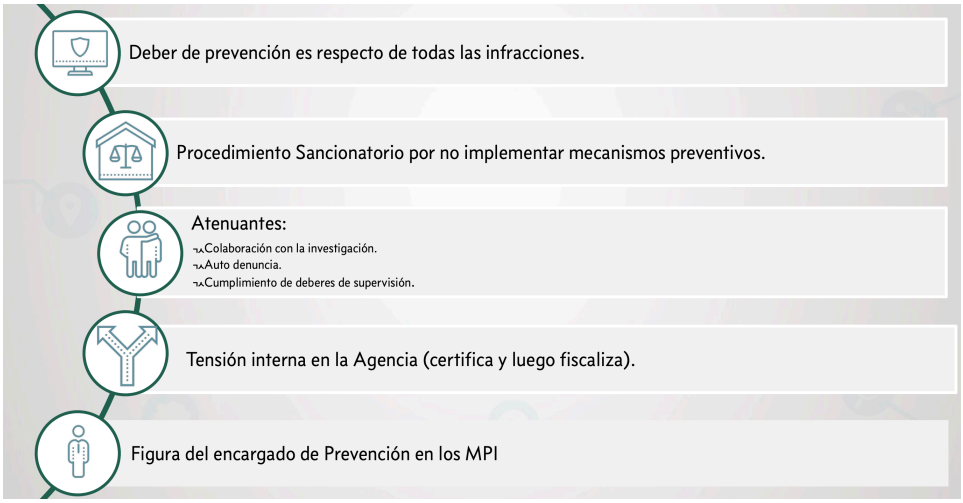

Figura 3: Principios que guian la normativa

VII. General Data Protection Regulation (GDPR UR)

Norma comunitaria vinculante de aplicacion directa a Estados Miembros de la UE (no requiere transposición). Entro en vigencia el **25 de mayo de 2018** y es importante por qué:

- Aplicación extraterritorial: fuera del territorio, es un reglamento generalizado.
- Marco de referencia internacional
- Decisión de adecuación: certificación de la unión europea

Figura 4: Normativa Internacional

VIII. Desafíos

a. Gobernanza de Datos

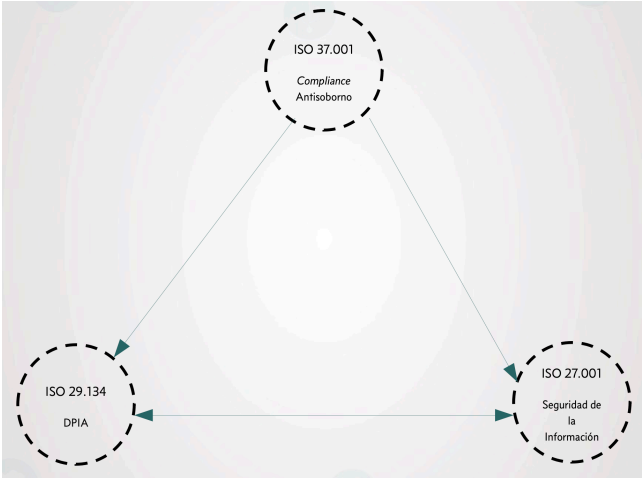

Figura 5: Normas técnicas vinculadas a la gobernanza de datos

b. Privacy by design

c. Data privacy impact assesment

d. Algorithm Accountability

Documento elaborado con las herramientas de Rmarkdown