



Privacidad de Datos Personales: La Experiencia de Chile

Stefan Larenas Riobó



Ley 19.628 sobre protección de la vida privada (LPVP)

- El artículo 19 N°4 de la Constitución Política de la República, que establece el respeto y protección a la vida privada y a la honra de la persona y su familia; y la Ley 20.575, «Ley Dicom», configuran el marco normativo fundamental en materia del derecho a la vida privada y protección de datos personales publicada el año 1999.

- En su origen esta ley tenía por objeto contribuir a disminuir el riesgo país, al asociarse el tratamiento de los datos con un instrumento orientado al orden público económico.
- Sin embargo, más que implementar un sistema de protección de datos personales lo que hizo, principalmente, fue regular el uso del dato económico.
- El resultado ha sido la instauración de un marco jurídico altamente permisivo, débil en cuanto a las posibilidades de control que pueden realizar tanto los titulares de datos como terceros y limitado en cuanto a la posibilidad de aplicar sanciones a las infracciones a los deberes que la ley establece.

ODECOU

ORGANIZACIÓN DE CONSUMIDORES Y USUARIOS

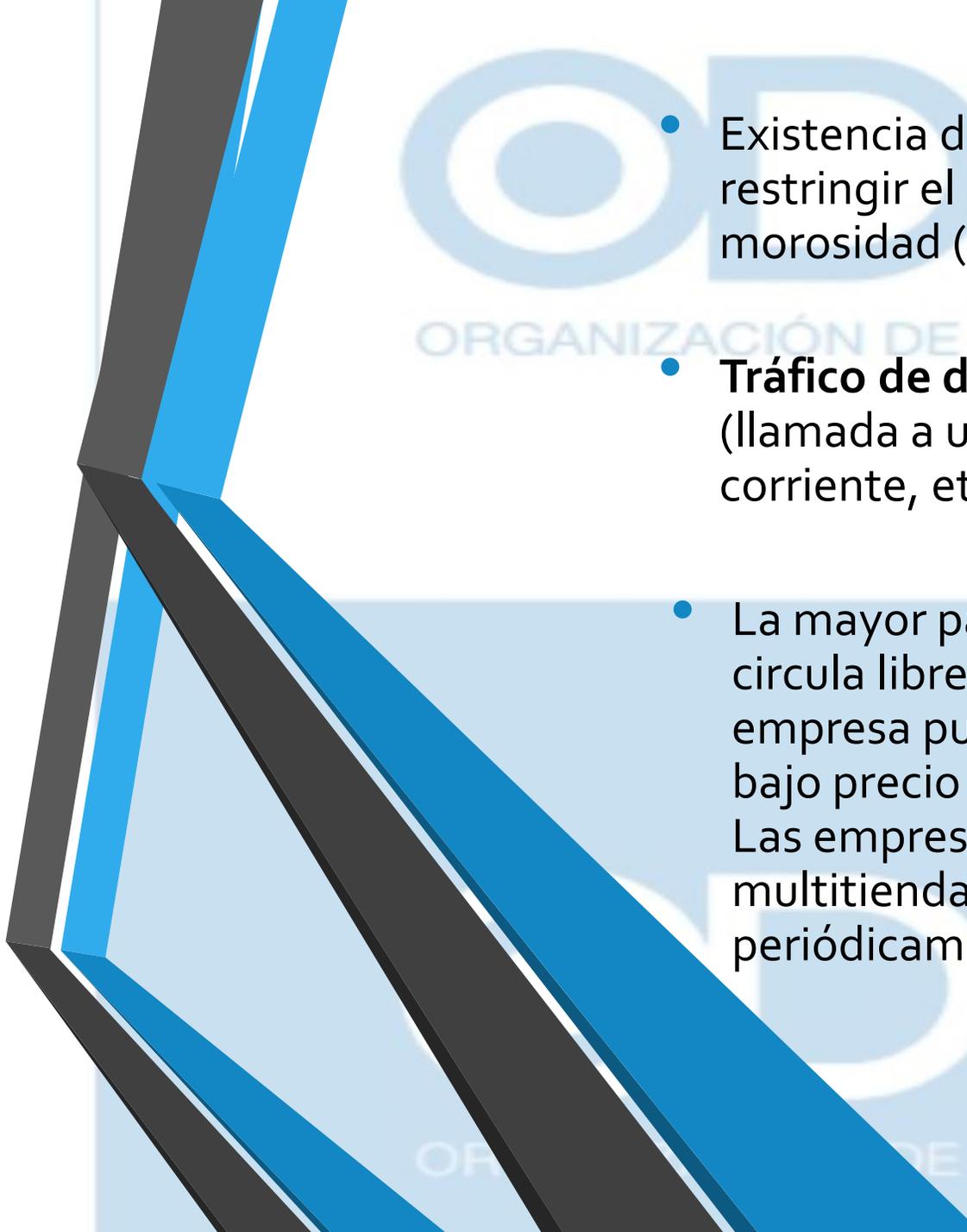
- Noción amplia de “tratamiento” de datos.
- Tratamiento de “datos personales” abarcando la mayor cantidad de operaciones posibles, como recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

ODECOU

ORGANIZACIÓN DE CONSUMIDORES Y USUARIOS

Consentimiento

- Art. 4° inciso primero: 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.
- Excepciones: No se requiere autorización del titular cuando sea tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial.
- Tampoco se requiere autorización cuando lo realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquello.

- 
- Existencia de «**listas negras**» en el mercado financiero para restringir el acceso al crédito a deudores con alta tasa de morosidad (DICOM).
- **Tráfico de datos** / mala práctica de venta de bases de datos (llamada a una persona ofreciéndole un servicio (seguro, cuenta corriente, etc.)
 - La mayor parte de la información personal- sensible o íntima- circula libremente por el mercado. Por alrededor de USD 160 una empresa puede acceder a bases de datos de números celulares. A bajo precio se venden millones de cuentas de correo electrónico. Las empresas de telecomunicaciones, comercios, bancos multitiendas y aerolíneas intercambian o adquieren periódicamente millones de datos personales.

- Gran debilidad: No hay un órgano competente a cargo de la fiscalización de esta regulación.
- Las infracciones a esta Ley son de competencia de los Juzgados Civiles, los cuales conocen y aplicarán la multa correspondiente.
- Multa de 68 a 680 USD.
- Multa de 680 a 3.400 USD si es información financiera. Indemnización de perjuicios en juicio sumario.

2012 - 2014

Por mantener a clientes repactados en DICOM: Corte Suprema declara admisible demanda contra Presto

21 de agosto de 2013



Share 8

Twitter 4

8+1 0

in Compartir

La acción judicial busca compensar el daño causado a todos los afectados por esta práctica, quienes, pese a ponerse al día con su deuda, fueron mantenidos en DICOM.

La Justicia declaró admisible la demanda contra Presto, por infringir a la Ley del Consumidor y la ley de Datos Personales, al mantener en Dicom a los consumidores que repactaron su deuda de manera voluntaria con la empresa, basados en una cláusula del documento que se les hizo firmar al reprogramar.



Dicha cláusula señalaba: "acepto que la suscripción de este documento no hace cesar la mora por lo que no conleva la eliminación de mis antecedentes comerciales y/o financieros sino hasta el pago de la última cuota". Es decir, aunque el cliente reprogramara la deuda y estuviera al día, se le mantenía en DICOM hasta que pagara el total.

Inicio » Economía » Consumo

08/12/2012 | ENVIAR | IMPRIMIR

LAS OTRAS "LISTAS NEGRAS" DE MOROSOS QUE EXISTEN ADEMÁS DE DICOM

Otras grandes empresas, conocidas como distribuidoras de deudas, operan en el mercado local. Están vinculadas a los gremios de la banca y del comercio, ofreciendo reportes de crédito a sus clientes sobre la base de los datos comerciales de consumidores.



Jueves 6 de diciembre de 2012 | por Roberto Valencia - foto: Archivo

Jueves, 27 de Marzo 2014

Investigan filtración de millones de datos del Registro Civil

50.481.298 registros para documentación de cédulas y pasaportes habrían sido copiadas el 12 de septiembre

Twitter 0 Like Be the first of your friends to like this.



La Unidad de Alta Complejidad de la Fiscalía Metropolitana Centro Norte comenzó una ronda de cuestionarios a funcionarios del Registro Civil luego de que se denunciara una masiva filtración de datos.

De acuerdo a información de Radio Cooperativa, el 30 de octubre de 2013, la directora subrogante del servicio, Claudia Gallardo, acusó que 50.481.298 registros para documentación de cédulas y pasaportes habían sido copiadas el 12 de septiembre, en pleno paro de los funcionarios.

En el Ministerio Público existirían dos líneas de investigación: una que apunta al Departamento de Informática del servicio y la otra a ex empleados de la anterior concesionaria, Sonda, reemplazada por la francesa Morpho.

TAMBIÉN RECOMENDAMOS

Martes, 24 de Febrero 2015
Oficinas del Registro Civil abrirán este sábado

En conversación con Radio Cooperativa, el CEO de Morpho, Philippe Petitcolin, descartó que la firma esté involucrada en los delitos.

LATERCERA Política Nacional Mundo Negocios Opinión Santiago Tendencias Educación Cultura Entretenimiento Deportes La Tercera TV

Opinión

Ingresar Suscripciones Club Edición Impresa

Síguenos

Editorial Correos de los Lectores Ideas Y Debates Representante del Lector

Tráfico de datos personales

No obstante existir un proyecto de ley aprobado transversal y unánimemente por la Comisión de Economía del Senado, que propone la implementación de las restricciones omitidas en 1999, cuesta entender que tanto la Administración pasada como en el contenido de un nuevo proyecto de ley se siga optando por regular con falta de idoneidad el tráfico de datos personales.

por Renato Jijena - 25/03/2013 - 04:00

Twitter 0 Recomendados 0 Post

EN CHILE, el tráfico anónimo e indiscriminado de bases de datos personales o nominativos es un tema antiguo. Buscando culpables de la cesión de datos a espaldas de los titulares y propietarios de sus antecedentes, se ha apuntado por ejemplo- contra las AFP, isapres, farmacias, servicios públicos, municipalidades, compañías de seguros, tiendas de retail y empresas de marketing directo, porque precisamente la materia prima de su negocio es la información nominativa, que mientras más fidelizada, mayor valor transaccional tiene. Nada debe extrañar que ahora se quiera crear alarma pública cuestionando a empresas de telefonía celular que operan bajo el amparo de la legislación vigente.

Claro ofrece pagar \$30.000 a más de 4 mil clientes por filtración de datos

La empresa reconoció que el 8 de julio quedó al descubierto una base de datos con información sensible de sus usuarios.

Emol

Viernes, 16 de Agosto de 2013, 11:38

Twitter 64

8+1 1

Me gusta 303



Foto: El Mercurio

SANTIAGO.- La empresa Claro compensará con \$30 mil a cerca de cuatro mil doscientos consumidores que se vieron afectados por una filtración de sus datos personales desde su sitio web, hecho ocurrido a principios de julio.

El compromiso se enmarca en una mediación colectiva, iniciada por el Sernac, tras recibir reclamos de consumidores que señalaban haber sido víctimas de una filtración de sus datos personales desde la página web de Claro.

Ante las denuncias, el servicio le remitió un oficio a la empresa para que le informara sobre lo ocurrido; el número de consumidores que se vieron afectados; y las medidas que adoptarían para resarcir a los clientes; entre otros aspectos.

En su respuesta, la empresa Claro reconoció que el pasado 8

RELACIONADOS

Haz tu widget <>

Azul Azul: Heller suma a ejecutivo del grupo Bethia y Sabino Aguad asume como gerente general

2016

CIPER CONSTATÓ QUE HACIA 10 MESES SE ALERTÓ A SEGURIDAD DEL MINSAL

Grave falla en la red del Minsal dejó expuesta información confidencial de pacientes

Por : [Víctor Carvajal](#) y [Matías Jara](#) en Reportajes de investigación
Publicado: 05.03.2016

COMPÁRTELO PUBLICALO SUSCRÍBETE A "REPORTAJES DE INVESTIGACIÓN"

Investigación Documentos asociados Comentarios (15)

Pacientes con VIH, mujeres que pidieron la píldora del día después, enfermos mentales. Todos con nombre, RUT y domicilio estaban disponibles hasta el viernes 4 de marzo en la plataforma computacional del Ministerio de Salud. Cualquiera de sus 100 mil funcionarios, e incluso externos, podían acceder a esa información privada. Se trata de la peor vulneración de la seguridad

5 de marzo 2016

LA TERCERA

Nacional

Entel descarta responsabilidad en la falla de seguridad del sistema informático del Minsal

El director de Asuntos Públicos y Relaciones Institucionales de la empresa, Felipe Simonsohn, sostuvo que "los controles de seguridad y acceso de los equipos no son de nuestra responsabilidad", ante la Comisión de Salud de la Cámara.

Lorena Leiva
15 de marzo del 2016 / 21:43 Hrs

0 | j | l | c | url | -A | +A

15 de marzo 2016

3 millones de datos de pacientes, con nombre, RUT y domicilio, con VIH, mujeres que pidieron la píldora del día después, enfermos mentales entre otros, expuestos en carpetas compartidas durante meses hasta el viernes 4 de marzo pasado en la plataforma computacional del Ministerio de Salud.

2016

¿SABÍA UD. QUE...? A los hombres en estado vegetal siempre los dejan plantados. Por:

THE CLINIC ONLINE

HOME PODER CHILEAN NEWS WEBEO COLUMNAS LA CALLE MUNDO DEPORTES CULTURA LA CARNE JUEGOS AROUND THE WORLD GA

Municipalidad de Ñuñoa publicó datos de paciente VIH en internet y culpó a Google del error

9 COMENTARIOS

Ricardo Ahumada | 15 Marzo, 2016 | Tags: ñuñoa, Chilean News, google, protección de datos, vih

Fotos: Agencia Uno

Compártelo Tuitéalo

Una vecina de la comuna que había pedido ayuda para un tratamiento médico se percató que la información estaba en la web y demandó al municipio por vulnerar la protección de la vida privada. La municipalidad respondió que esto se debía a un lamentable error y se excusó señalando que “fue Google quien a través de sus motores de búsqueda, sacó y exhibió la información personal” de la demandante. Tras un fallo en primera instancia, ahora la Corte de Apelaciones deberá resolver si se paga o no la indemnización por daño moral a la demandante.

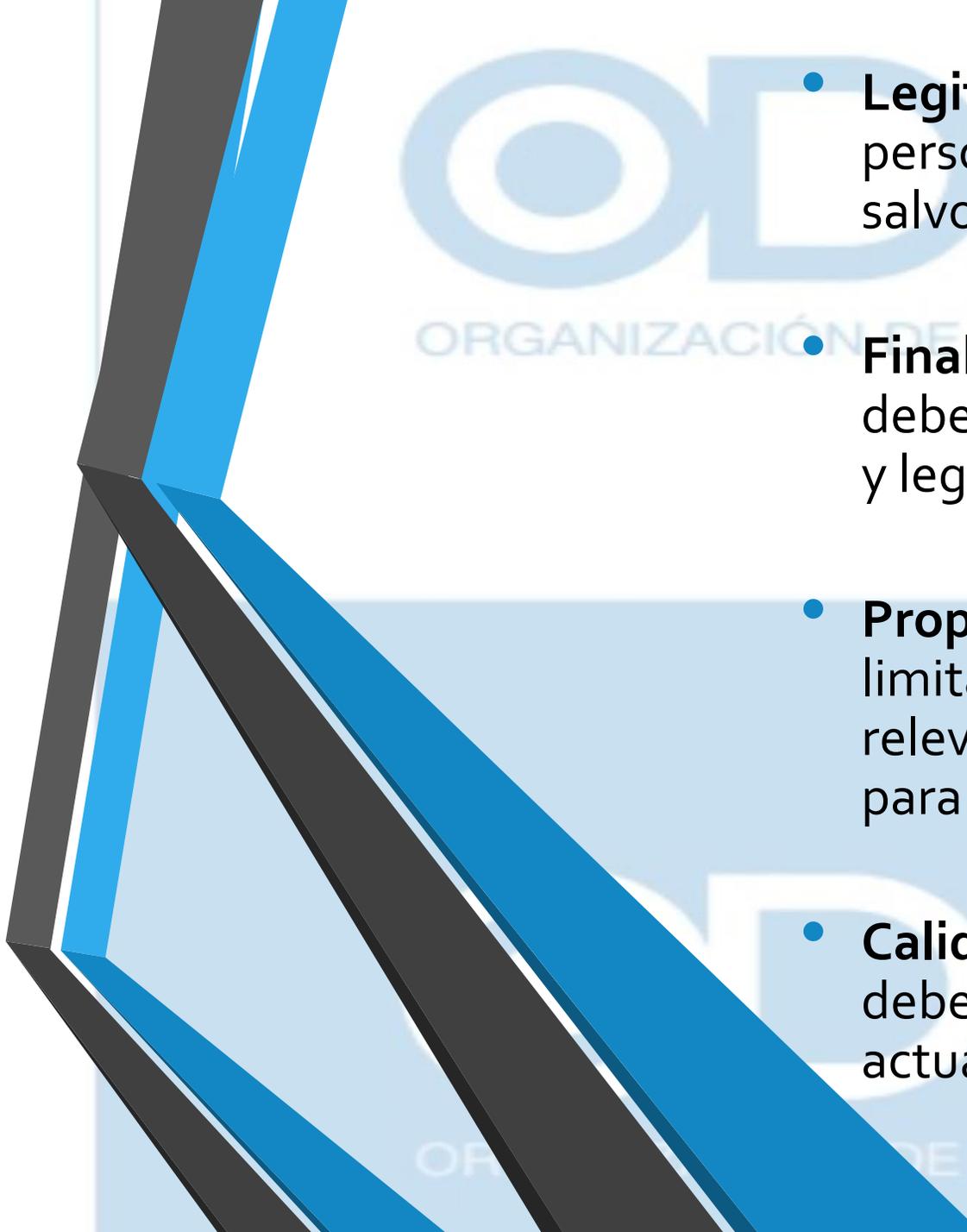
El 5º Juzgado Civil de Santiago condenó el 2 de octubre de 2015 al municipio tras establecer *“el tratamiento indebido que la demandada dio a los datos personales entregados al departamento de Desarrollo Comunitario de la I. Municipalidad de Ñuñoa, en lo referente a ser portadores del VIH, el cual es considerado un dato sensible de acuerdo a lo dispuesto en el artículo 2º de la Ley 19.628”*.

Además, el fallo desestimó atribuirle la culpa a Google porque fue a la municipalidad *“a quien los actores entregaron los datos y como responsable de los registros o bases donde se almacenan estos datos, es responsable de cuidar de ellos con la debida diligencia, todo ello como versa el artículo 11 de la ley 19.628”*.

15 de marzo 2016

Disposiciones Generales: Proyecto nueva Ley

- Definición del objeto de la ley, incorporando la tendencia internacional de reconocer la protección de datos como el derecho de las personas de controlar y proteger la información de la cual son titulares, de manera de lograr el resguardar los derechos fundamentales.
- El ámbito de aplicación de la ley, para lo cual centra la protección en los datos personales, independientemente de si se encuentran o no en una base de datos, del soporte en que éstas se contengan o si el tratamiento de los mismos los realizan órganos del Estado, particulares o personas naturales.

- 
- Legitimidad:** Sólo pueden tratarse los datos personales cuando el titular de los mismos consienta, salvo que medie una excepción legal.
- Finalidad:** En cuya virtud en tratamiento de datos debe limitarse a finalidades determinadas, explícitas y legítimas.
- Proporcionalidad:** El tratamiento de los datos debe limitarse a aquellos que resulten adecuados, relevantes y no excesivos en relación con la finalidad para la que se recolectaron.
- Calidad:** Por la cual el responsable del tratamiento debe asegurar que los datos que trata son exactos, actuales y completos.

- **Transparencia:** El responsable del tratamiento deber tener políticas claras, legibles y en castellano sobre las operaciones de tratamiento de datos que realiza.
- **Responsabilidad:** El responsable del tratamiento debe adoptar las medidas que permitan asegurar que cumple con los principios y normas sobre tratamiento de datos y contar con los medios que le permitan demostrar a los titulares de datos y a las autoridades que ello es así.
- **Seguridad:** Por la que debe adoptar las medidas para evitar que el tratamiento de datos cause daños, debiendo considerar el riesgo implícito en el tipo de datos que trata.

- El proyecto garantiza los derechos de acceso, rectificación, cancelación, oposición e impugnación de valoraciones personales.
- De estos derechos sólo es desconocido en Chile al día de hoy el derecho a la impugnación de valoraciones personales. Con él se busca que no se adopten decisiones en contra de las personas basadas únicamente en el tratamiento de datos personales, de manera de minimizar las estigmatizaciones y discriminaciones fundadas en información que puede adolecer de problemas de calidad.
- Innovaciones en este punto en lo que ha sido la experiencia nacional, representando una significativa evolución de la protección de los derechos fundamentales en la materia es el hecho de que se establece que los derechos señalados son irrenunciables y que no pueden ser limitados por pacto o convención alguna.

Datos especialmente protegidos

- El proyecto reconoce que hay ciertos tipos de datos que requieren de condiciones especiales para su tratamiento, por la vía de cuidados especiales para el otorgamiento del consentimiento del titular, obligaciones de seguridad o autorización previa de la autoridad de protección de datos.
- Entre ellos se encuentran los datos personales sensibles, los relativos a infracciones civiles, penales o administrativas, a la salud, a las telecomunicaciones, a los datos biométricos y a los menores de edad.

Registro Nacional de Bases de Datos

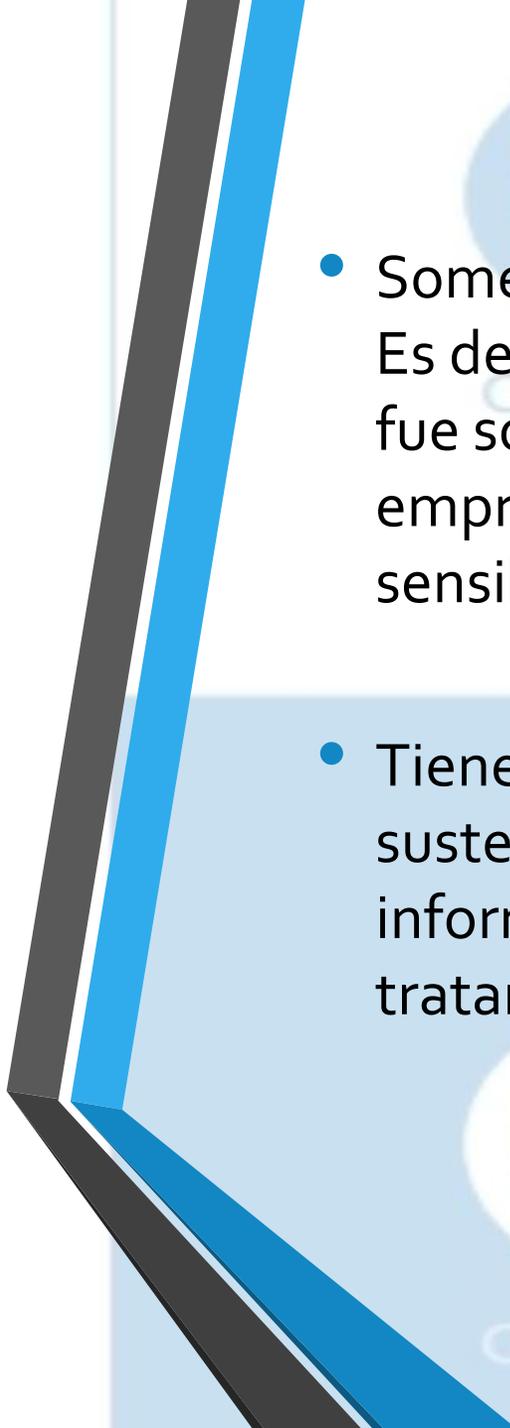
- Con la ley (por ejemplo las transferencias internacionales o los códigos deontológicos).
- No se almacena la base de datos propiamente tal, sino que información relativa a la misma, de manera que los titulares de datos puedan acudir al Estado a conocer dónde pueden estar sus datos y, junto a ello, se pueda realizar una mejor fiscalización de las bases de datos existentes. Uno de los mayores problemas que tienen las personas para controlar y proteger su información es que no saben dónde se encuentra.
- Adicionalmente, se establecen reglas para que los órganos del Estado puedan intercambiar información de las personas de manera de prestar servicios integrados a los ciudadanos.

Nueva Institucionalidad: Consejo para la protección de datos

- El proyecto crea la autoridad de protección de datos, bajo la fórmula de una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio.
- Velando cumplir con las exigencias que la UE exige a esta clase de organismos para poder lograr el reconocimiento de país seguro y poder garantizar la transferencia Chile-Europa-Chile de datos personales.
- Las funciones del Consejo es posible agregarlas bajo la promoción, fiscalización y sanción.

Infracciones y sanciones

- El Proyecto considera infracciones leves, graves y muy graves, dependiendo del grado de afectación o amenaza de los derechos fundamentales de los titulares de datos.
- Las sanciones que se consideran para cada tipo de infracción son de multas, sin embargo para infracciones calificadas como graves o muy graves en que haya reincidencia es posible además inhabilitar la base de datos. La cuantía de las sanciones se gradúa atendidos ciertos criterios que da la ley (por ejemplo carácter continuado de la infracción, beneficio obtenido por el infractor, reincidencia, grado de intencionalidad, etc.)
- Las sanciones son aplicadas por la autoridad de protección de datos, a través de un procedimiento en sede administrativa que garantiza el debido proceso y siendo posible apelarlos ante la Corte Suprema bajo las normas del recurso de amparo.

- 
- 
- Sometido a **Consulta Ciudadana** entre el 25 de julio y 22 de agosto de 2014. Es decir, incluso antes del ingreso del proyecto de ley, el borrador de éste fue sometido al escrutinio público, para recibir opiniones del sector privado, empresas, académicos, etc. Se notó una gran cantidad de observaciones y sensibilidades especialmente del sector empresarial.
 - Tiene por objetivo dar forma a un Sistema de Protección de Datos sustentado en el derecho de las personas de controlar y proteger su información, de manera de evitar que sus derechos sean afectados por el tratamiento de datos.
- 
- ORGANIZACIÓN DE CONSUMIDORES Y USUARIOS



GRACIAS

