UNIVERSIDAD FINIS TERRAE
FACULTAD DE DERECHO
ESCUELA DE DERECHO

PROTECCIÓN DE LOS DATOS PERSONALES EN CHILE, SU TRATAMIENTO Y COMERCIALIZACIÓN

Análisis y críticas a la ley N° 19.628.

SEBASTIÁN ANDRÉS LABBÉ IBARRA

PAULA FERNANDA LATRILLE GONZÁLEZ

Memoria presentada a la Facultad de Derecho de la Universidad Finis Terrae para optar al Título de Licenciado en Ciencias Jurídicas y Sociales

Profesora Guía: María Rebeca Ahumada Durán

Santiago, Chile

2018

Contenido

INTRODUCCIÓN

La evolución tecnológica impulsada por las dos guerras mundiales produjo avances importantes en la telefonía y los primeros hitos en la era computacional. En el siglo XX evolucionó internet y las tecnologías, hasta reducirse significativamente sus costos, transformándose en accesibles para casi todas las personas. La informática y las telecomunicaciones se transformaron en elementos esenciales de la vida occidental, pero también en mecanismos potencialmente contaminantes para el disfrute de la libertad y la igualdad que las constituciones contemporáneas reconocen a sus ciudadanos, pues hoy en día vivimos en la llamada "Sociedad de la información", en la que la fusión de la informática y la industria de las telecomunicaciones (que convergió en "las tecnologías de la información y la comunicación") se ha mostrado como uno de los sectores más dinámicos y de mayor crecimiento en la economía mundial,[1] tecnologías que nos permiten mayor conectividad entre nosotros, pero que a la vez nos perjudican. A medida que navegamos por internet o interactuamos a través de medios automatizados ya sea con personas o empresas, hacemos entrega de información que, si se relaciona a una persona natural determinada o determinable produce una cantidad innumerable de datos personales.

Muchas cosas son consideradas datos personales. Desde cosas tan esenciales, como lo son los atributos de la personalidad como el nombre, domicilio, nacionalidad, llegando tan lejos como es el número de tarjeta de crédito, patente del auto y otras cosas que uno comparte constantemente en sus redes sociales como son los gustos musicales, ideológicos y de opinión general. La información que ingresemos a Internet será un dato personal siempre que con ella seamos identificados. Muchas veces a un solo clic, das el consentimiento para que tu información sea tratada, almacenada, recopilada y vendida, de manera libre por

[1] ANGUITA RAMÍREZ, Pedro. La protección de datos personales y el derecho a la vida privada. Editorial Jurídica de Chile, Santiago, Chile, 2007, pág. 627.

estas empresas u organismos, a través de los términos y condiciones que rara vez leemos.

La protección de los datos personales tiene su origen en el derecho constitucional de la intimidad o privacidad y este a su vez, empezó a construirse a mediados del siglo XIX cuando aparecieron las primeras amenazas a la esfera privada. El derecho a la privacidad y la vida privada en Chile fue incorporado recién con la Constitución de 1980 como una garantía fundamental, establecida en el artículo 19° número 4° que consagró "El respeto y protección a la vida privada y pública y a la honra de la persona y su familia.", siendo a primera vista muy escueto e insuficiente y tardío en relación con otros países.

La protección de los datos personales nació como un aspecto de la intimidad, pero posteriormente algunos países lo han desarrollado de manera más profunda como dos derechos constitucionales distintos. El llamado "derecho a la protección de datos", o "derecho a la autodeterminación informativa", es un derecho de tercera o cuarta generación, siendo su bien jurídico la libertad informática y persigue garantizar a cada una de las personas un poder de control y disposición sobre los datos que les afectan, sean íntimos o no, públicos o privados, para preservar la propia identidad, dignidad y libertad.[2]

Fue en el año 1999 que se publicó la Ley 19.628 sobre protección de la vida privada, con el subtítulo de protección de datos personales, siendo la primera ley de América Latina en datos personales, la cual no terminó con la comercialización de los datos personales de los ciudadanos chilenos. Además, con el transcurso de los años y de la tecnología entre otras cosas, se ha vuelto poco eficaz para proteger a las personas, como la doctrina incesantemente lo ha señalado.[3]

Todos los datos que son recopilados pueden generar un perfil detallado sobre nosotros, ejemplo de esto es lo que realizan las empresas y comercios al pedirnos nuestro número de identificación (RUT) cada vez que realizamos una compra,

[2] DE LA SERNA BILBAO, María Nieves. La institucionalización de la protección de datos de carácter personal. En: Reflexiones sobre el Uso y Abuso de los Datos Personales en Chile. Santiago: Expansiva, 2011. Pp. 55-77.
[3] Pedro Anguita Ramírez; Raúl Arrieta Cortés; Alberto Cerda; Renato Jijena.

señalando que es para acceder a descuentos o beneficios, pero al darlo de manera voluntaria, accedemos a que además se cruce información que les permite recabar un perfil de nuestros gustos, intereses, intimidad, es decir un perfil como consumidor para realizar campañas publicitarias cada vez mas personalizadas para los distintos públicos, muchas veces prediciendo hasta enfermedades o qué productos podrían ser atractivos, antes que nosotros los sepamos.[4]

El objetivo del presente trabajo es realizar un análisis del sistema general de protección de datos personales de Chile, señalar sus falencias y hacer una reflexión y crítica a los abusos que se generan en el sistema Chileno principalmente por las entidades que se dedican a comercializar los datos de las personas, pues como es sabido, la información es poder, por lo tanto, poseer un perfil detallado de cada uno de nosotros sobre lo que comemos, compramos, pensamos, leemos, etc., constituye una gran amenaza a nuestras garantías fundamentales. Sin embargo, antes de eso haremos de la manera más sintetizada posible un capítulo sobre los inicios de los datos personales y su historia.

[4] Datos Protegidos [en línea]: ¿Eres un producto? [fecha de consulta 28 de septiembre de 2018]. Disponible en: < https://datosprotegidos.org/no-doy-mi-rut/>

CAPÍTULO 1

EVOLUCIÓN HISTÓRICA DE LOS DATOS PERSONALES Y SU PROTECCIÓN

1) Evolución histórica

Los precursores en este tema fueron Alemania y Suecia, incorporándose paulatinamente a la tendencia de regular la protección de los datos personales, el resto de los países de Europa Occidental. La tendencia mundial ha sido a desarrollar el tema a través de la vía legislativa, mientras otros países optaron por la vía constitucional.

La primera ley de datos personales fue aprobada por el parlamento de Land Hesse, Estado de Alemania, en 1970. Esta ley nació como una protección a los ciudadanos, luego de que las autoridades buscaran aumentar la eficiencia de la administración, automatizando los procesos. Fue la primera ley en el mundo en regular los datos personales en poder de los órganos públicos y buscó proteger los datos personales y su tratamiento con el Estado, el cual era regulado por un Comisario Federal que establecía la fiscalización y el correcto tratamiento de los datos. Esta ley fue de vital importancia debido a que fue la base para promulgar la Ley Federal Alemana de 1977 (Bundesdatenschutzgesetz), que incorporó y mejoro el tratamiento de los datos personales.

Suecia también, promulgó una ley buscando proteger los datos personales, mediante la Data Lag de 1973, a través de la cual se impone un sistema de registro abierto para publicitar los bancos de datos personales relativo a personas físicas realizado por medios automatizados, los que debían ser previamente autorizados para funcionar, relacionado con la autoridad de control de la Datainspektionen (expresión del Ombudsman, figura legal de los países escandinavos que actúa como Defensor del Pueblo, representándolo y velando por sus intereses), que fiscalizaba el tratamiento de datos y se encargaba de que se respetara debidamente

la ley con facultades inspectoras, normativas y procesales para requerir la aplicación judicial de sanciones.

Luego de estas primeras leyes, vino una segunda generación; leyes que buscaban mejorar la calidad de la transmisión de los datos, en la cual además se comenzó a regular y tratar los “datos sensibles”. Es en esta generación que se buscó delimitar el derecho a la autodeterminación informativa, mediante el reconocimiento y la tutela de los derechos de acceso y control de las informaciones. La autodeterminación informativa o libertad informática se refiere básicamente al derecho que tienen las personas saber, controlar y definir la información que existe sobre ellos mismos.

Siguiendo la tendencia de incorporar la Autodeterminación Informativa al derecho positivo, se encuentran las primeras consagraciones constitucionales de este derecho fundamental; en la Constitución de Portugal del año 1976, se establece en su Artículo N°35 que; *“todo ciudadano tiene derecho a tener conocimiento de los datos que constan en ficheros y registros informáticos que le afecten y de la finalidad a que se destinen estos datos”.* A su vez, en la Constitución de España del año 1978 se incorpora una norma relacionada, en el artículo N°18.4 que establece*: “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicios de sus derechos.”*

La tercera generación de leyes sobre datos personales, tienen el desafío de afrontar los avances de la informática y de las técnicas legislativas, todo esto derivado de la Autodeterminación Informativa. En esta generación se trata de unificar y armonizar los principios fundamentales y la regulación de los datos personales, para un mayor ahondamiento y comprensión en la materia, lo analizaremos tanto en la situación a nivel mundial y regional, del continente de América y Europa y finalmente en nuestra legislación.

2) Situación Mundial:

En el ámbito mundial el primero en legislar sobre esta materia, fue la Organización para la Cooperación Económica y el Desarrollo, también llamada OCDE en atención a sus iniciales. La OCDE es un organismo de cooperación internacional y su principal objetivo es la coordinación y análisis de las políticas públicas y sociales, buscando fomentar la expansión del comercio entre sus 37 países miembros. Chile y Colombia son los únicos países sudamericanos que pertenecen a este organismo, nuestro país desde el año 2008 y Colombia desde este año en curso.

En la década de los 70, la OCDE realizó foros de discusión e investigación para evitar que se crearan barreras proteccionistas en el comercio internacional por la falta de unificación y armonía entre las leyes de datos personales de cada país. Dichas investigaciones arribaron a la “Recomendación relativa a las directrices aplicables a la protección de la vida privada y a los flujos transfronterizos de datos personales” del año 1980. Los contenidos de aquella investigación y los consensos alcanzados sirvieron de base esencial para que la Asamblea General de la ONU (Organización de Naciones Unidas), estableciera un contenido mínimo que debieran contener las leyes, a través de la Resolución 45/95, adoptada en el año 1990 por la misma Asamblea, llamada “Principios Rectores para la Reglamentación de los ficheros computarizados en datos personales”.

Es importante destacar en esta materia que los autores y miembros de las comisiones que sirvieron para promulgar las Directivas y Resoluciones por la Asamblea General de la ONU fueron los mismos que participaron en el Convenio 108 de 1981 realizado por la Comunidad Europea, el cual es analizado en el punto siguiente sobre la Situación Regional en Europa.

En la sesión mencionada N°45 del año 1990, se establecieron los principios que serían la base para la normativa en cuanto a la protección de datos a nivel mundial y se clasificaron en dos grandes grupos[5];

2.1) Principios adoptados en la Resolución 45/95 de la ONU del año 1990 *relativos a las garantías mínimas que deberían preverse en la legislación nacional*;

- Principio de Licitud y Lealtad: Busca que los datos no sean tratados de manera ilícita o desleal y que tampoco vayan en contra de los principios de la Carta de las Naciones Unidas.

En términos generales se refiere a que no se produzcan discriminaciones arbitrarias para el titular de datos, desarrollándose el tratamiento de datos con sujeción a los principios, normas nacionales e internacionales, además de los derechos de las personas.

- Principio de Exactitud: Quienes almacenen y traten los datos personales deben cerciorarse de que estos sean exactos y que se actualicen de manera periódica o cuando se utilice la información contenida en un expediente.

- Principio de Finalidad: Todo tratamiento de datos personales se debe limitar al cumplimiento de las finalidades determinadas al momento de su creación. La persona responsable del tratamiento de datos solo puede realizar tratamientos compatibles con las finalidades para las cuales obtuvo el dato. Debe informar a terceros y a la persona interesada que estos datos siguen siendo pertinentes a la finalidad perseguida y que no serán utilizados o revelados sin el consentimiento de la persona interesada. Además, el período de conservación no puede exceder del necesario para alcanzar la finalidad con la cual se ha registrado.

- Principio de Acceso a la persona interesada: Se refiere a que la persona interesada tiene derecho a saber si se está procesando información que les concierne y

[5]Resolución 45/95, 14 diciembre 1990. [en línea]: Principios rectores para la reglamentación de los ficheros computarizados de datos personales. [fecha de consulta: 4 de octubre de 2018]. Disponible en: <http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf>

conseguir acceso a ella sin demoras y obtener rectificaciones o supresiones cuando estos datos sean ilícitos, injustificados o inexactos, existiendo un recurso para precaver algunas de estas situaciones y hacer valer de manera plena el derecho.

- Principio a la no discriminación: Sin perjuicio de las excepciones previstas, este principio consagra que no deben registrarse datos que puedan originar una discriminación ilícita o arbitraria, en particular información sobre el origen racial, color, vida sexual, opiniones políticas, condiciones religiosas o filosóficas y respecto de la afiliación a ciertos organismos o sindicatos.

- Facultad de establecer excepciones: Solo se pueden hacer excepciones a los principios anteriormente mencionados (del número 1° al 4°) si son necesarios para proteger la seguridad nacional, el orden público, la salud, la moral pública y en particular los derechos y libertades de los demás. Estas excepciones se deberán prever expresamente por la ley. Respecto a las excepciones del Principio N°5 también se deberá hacer la excepción por una ley previa y se podrá autorizar solo dentro de los limites previstos por la Carta Internacional de los Derechos Humanos y demás instrumentos pertinentes en materia de protección de los derechos contra la discriminación.

- Principio de Seguridad: Se refiere a que el responsable de la base de datos debe adoptar todas las medidas de protección contra los riesgos naturales y humanos tales como el acceso sin autorización, la utilización encubierta de datos y contaminación por virus informáticos.

- Control y Sanciones: Cada legislación deberá asignar a la autoridad que se encargue de controlar el respeto por estos principios, ofreciendo garantías de imparcialidad, independencia con respecto a las personas, organismos responsables del procesamiento de los datos y de su aplicación, estableciendo sanciones penales y de otro tipo, como recursos individuales apropiados en caso de contravención.

- Flujo de datos a través de las fronteras: Para que la información entre países pueda circular de manera libre, la legislación de datos personales deberá ofrecer garantías comparables de la protección de la vida privada, agregando como amplia excepción, que cuando no haya garantías comparables no se podrán imponer limitaciones injustificadas a dicha circulación siendo solo la medida que lo exige la protección de la vida privada.

- Campo de Aplicación: Los principios se deberán aplicar a todos los ficheros computarizados tanto públicos como privados, asimismo a los manuales.

2.2) Y *aplicación de los principios rectores a los ficheros de las organizaciones internacionales gubernamentales que contienen datos personales*.

Se refiere a que los principios antes señalados deberán ser aplicables a las organizaciones internacionales gubernamentales de datos personales, a reserva de las adaptaciones necesarias para tener en cuenta las posibles diferencias que puedan existir entre los ficheros con fines internos y los ficheros con fines externos relativos a terceras personas relacionadas con la organización. Además, señala que cada organización deberá designar a la autoridad que estatutariamente será competente para velar por la correcta aplicación de estos principios rectores.

Como última disposición, la asamblea acordó una cláusula humanitaria donde estipuló que deberá precaverse de manera específica una excepción a estos principios cuando el fichero tenga por finalidad proteger los derechos humanos o se deba prestar ayuda humanitaria.

Los principios mencionados anteriormente, son aplicables a todo tratamiento de datos en donde la normativa haya incorporado el derecho a la autodeterminación informativa. No pueden dejar de estar presentes para que exista plenamente este derecho.

Cabe señalar que estos principios fueron incorporados por la Legislación Chilena de Datos personales, la Ley N° 19.728 o Leges Data como indistintamente la

mencionaremos a lo largo de este trabajo. Luego analizaremos si estos principios son efectivamente recogidos por la legislación chilena y si de manera efectiva o no.

3) Situación Regional en Europa:

Es importante mencionar la situación del continente europeo, pues son los verdaderos pioneros en la búsqueda de unificar las normas de protección de datos personales. Mencionaremos dos normas trascendentales no solo para Europa, sino para el mundo en general.

3.1) Convenio 108 adoptado por la Comunidad Europea en 1981:

La importancia de este convenio radica principalmente en que es el primer instrumento internacional que busca reglar y normar el fenómeno del tratamiento automatizado de datos que pertenecen a personas naturales, todo esto visto desde una arista que trasciende la legislación interna de cada país pues el contenido de este buscaba uniformar a las diversas legislaciones europeas que fueron promulgadas durante la década de 1980, buscando realizar una normativa eminentemente comunitaria para poder hacer frente a la proliferación de leyes nacionales que pudiesen afectar su armonización.

La aplicación de este convenio en cuanto al procesamiento de datos iba desde el almacenamiento llegando hasta el borrado de este, el cual se daba tanto en el sector público como privado, con tal de que se refiriese a personas naturales y fuese realizado por medios informáticos. Sin desmedro de lo anterior, el convenio también admitía que los Estados miembros de manera facultativa pudiesen extender sus disposiciones a grupos de personas que contaran o no con personalidad jurídica, así como a los datos personales que fueren objeto de tratamiento no automatizado.

Uno de los principales aportes de este Convenio, fue su preocupación sobre el desafío que propone el flujo internacional de datos de carácter personal. Esto se realiza mediante una suerte de homologación que busca disponer una protección equivalente en la legislación aplicable a quienes participaban en la transmisión de datos, para así evitar que las partes hicieran una mala o errónea aplicación de la normativa de cada Estado parte.

Vale destacar que el mismo convenio hace mención del "Auxilio mutuo a los Estados partes", para cuyos efectos supone la existencia de una o varias autoridades en la legislación interna de cada uno de ellos, buscando así la cooperación institucional entre ellos, como la asistencia a los interesados que sean residentes en el extranjero en el ejercicio de sus derechos.

Para que efectivamente se produjera lo explicado anteriormente los Estados Partes del Convenio se comprometieron a adoptar en su normativa interna las medidas que fuesen necesarias para poder dar cumplimiento a los principios fundamentales de protección de datos que se adscribieron en el instrumento. Así sucedió en el caso de España y del Reino Unido.

3.2) Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de carácter personal (LORTAD):

Esta ley fue adoptada por España en año 1992 y es de vital importancia analizarla, porque fue la principal inspiración para nuestra legislación en cuanto a protección de datos personales.

España fue pionero en consagrar en su Constitución en el año 1978, en su artículo 18° inciso 4 que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Pero aquella temprana declaración constitucional, no se concretó en la adopción de una pronta legislación sobre protección de datos personales, pues aquello se hizo efectivo recién 14 años después con la Ley Orgánica 5/1992, "de regulación del tratamiento automatizado de los datos de carácter personal", popularmente conocida como LORTAD publicada el 29 de octubre de 1992.[6]

[6] SUÑE LLINAS, Emilio. Tratado de Derecho Informático: Introducción y protección de datos personales. "Sobre las primeras iniciativas parlamentarias en la materia". MADRID. Universidad Complutense, Servicio de Publicaciones. Año 2000. Volumen 1.

La doctrina española consideró tarde el cumplimiento del mandato del constituyente, además de encontrarla deficiente por la dependencia de la autoridad de control del gobierno y por sus limitaciones. Aquella protección a los datos personales que fue incorporada por España tempranamente en su constitución, pese a la poca aplicación práctica que tuvo debido a que no se contaba con el marco legal para poder ejecutar la protección, marcó un precedente a nivel mundial.

La LORTAD fijó los principios relativos al tratamiento de los datos personales: calidad, información, consentimiento, datos especialmente protegidos, datos de salud, deber de secreto, seguridad y cesiones, así como los derechos de las personas: acceso, rectificación, cancelación e impugnación de valoración.[7] Asimismo, la LORTAD luego fue complementada con dos normas reglamentarias: el Real Decreto 1332/1994, de 20 junio, por el que se desarrollaron diversos preceptos; y el Real Decreto 994/1999, de 11 de junio, sobre medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. En la actualidad ambas están derogadas. La actual ley española es la Ley Orgánica 15/1999, de protección de datos de Carácter Personal, abreviada LOPD, LOPDP o LOPDCD.

Es importante destacar que la LORTAD creó la denominada "Agencia de Protección de Datos" que más adelante pasaría a llamarse "Agencia Española de Protección de Datos", encargada de sancionar con multas a los que transgredan estos derechos, criticándose la alta cuantía de estas. Adelantamos que contrario a España y la mayoría de los países europeos, Chile no cuenta con un órgano homologo y autónomo con funciones fiscalizadoras, pese a que la ley chilena se inspiró en aquella.

3.3) Reglamento General de Protección de Datos como Modelo a seguir

En este punto tratamos el Reglamento General de Protección de Datos (RGPD o GDPR) (Reglamento 2016/679), por el cual el Consejo de la Unión Europea y la

[7] XX Aniversario de la LORTAD: 20 años de Protección de Datos. Diario Jurídico Español. MADRID, España. 6 de noviembre del 2012. Columna de Actualidad por Javier Sempere.

Comisión Europea tuvieron la intención de reforzar y unificar la protección de datos para todos los individuos dentro de la Unión Europea. Fue adoptado el 27 de abril de 2016 y entró en vigor a partir del 25 de mayo del presente año. Su objetivo principal fue dar control a los ciudadanos y residentes sobre sus datos personales y simplificar el entorno regulador de los negocios internacionales unificando la regulación dentro de los países miembros. El GDPR sustituirá a la Directiva de protección de datos (oficialmente Directiva 95/46 / CE) de 1995, pero a diferencia de la directiva, no obliga a los gobiernos nacionales a aprobar ninguna legislación habilitante, por lo que es directamente vinculante y aplicable[8].

Con esta norma se busca proteger los Datos personales incorporando nuevos tipos de datos como lo son las video llamadas, audios, fotografías y georreferencia. Señala también datos que estarán especialmente protegidos; los Datos Genéticos, Raciales y de Orientación Sexual entre otros.

El GDPR se aplicará en toda la Unión Europea, es decir será de ámbito territorial, lo cual amplía su aplicación respecto de la legislación anterior y pone especial énfasis en donde se encuentra la persona, no el tratamiento de datos o entidad pertinente. Es decir, si una empresa chilena tiene oficina en París, estará sujeta a esta legislación, y si tuviese oficina en Santiago, pero tuviera un operador de datos en territorio europeo se le aplicará de igual manera. Un ejemplo distinto, es el caso del turista australiano que comparte una foto desde Roma, también se le haría aplicación de la GDPR, es por esto último que la aplicación territorial será uno de los puntos más importantes de esta legislación a analizar, porque con esto se incluirá, por ejemplo, a Facebook que también tendría que cumplir y adaptarse a la legislación para poder seguir operando en territorio europeo.

Los puntos claves del RGPD son cinco y los analizaremos a continuación:

[8] Power data. [en línea]: “GDPR. Lo que debes saber sobre el reglamento general de protección de datos”. 2018. [fecha de consulta: 3 de octubre de 2018] disponible en: <https://www.powerdata.es/gdpr-proteccion-datos>

1. Situación de los Menores: Para los menores de 16 años respecto al tratamiento de datos personales no podrán consentir solos, tendrán que hacerlo sus respectivos padres o en su defecto tutores, todo esto para resguardar al menor.

2. DPO o Delegado de Protección de Datos: Se establece como obligación de los organismos públicos y respecto a empresas de gran escala o que traten datos sensibles. Las empresas que tengan menos de 250 trabajadores no tendrán que llevar registro.

3. Consentimiento: El cual tiene que manifestarse es decir debe ser expreso, también debe ser informado e individual y tiene que poder probarse su recepción. Consiste en explicar de manera sencilla al ciudadano, para qué serán usados sus datos personales, con qué fines y por cuánto tiempo y quien será el responsable de este tratamiento. Si los datos se van a usar para distintos fines, entonces se tendrán que pedir consentimientos de manera separada para cada tipo de dato.

4. Derecho al Olvido: Esta incorporación es novedosa a la legislación y consiste en el derecho de supresión el cual solo se había manifestado en sentencias judiciales, pero por primera vez en una ley. Consiste en que una persona puede solicitar la eliminación de sus datos a una empresa u organismo público, cuando este quiera retirar su consentimiento, cuando se han utilizado de manera ilícita o cuando se consideran innecesarios.

5. Portabilidad y Limitación: Son incorporados a los ya consolidados Derechos ARCO. La Portabilidad que había sido tratada anteriormente por la LOPD, permite a una persona pedir, recibir y transferir sus datos de una entidad a otra. Además, se incluye la Limitación que consiste en una suspensión temporal del tratamiento de datos para poder demostrar un interés legítimo o para resolver una disputa.

En cuanto a la fiscalización del GDPR, se le exige a cada Estado miembro de la Unión Europea que tenga una autoridad y que estas tienen que cooperar entre los otros estados y respecto a la Comisión Europea. Conjunto al GDPR, se crea el Comité Europeo de Protección de Datos, el cual se encargará de que el reglamento se aplique de manera coherente en todos los estados miembros, cuyas decisiones serán vinculantes. Por último, se incorpora todo tipo de sanciones pasando por advertencias, apercibimientos, medidas concretas y multas administrativas de hasta 10 millones de euros o, en su defecto, de hasta el 2% del volumen de negocio anual si se trata de una empresa.

Esta normativa es a nuestro juicio un buen modelo a seguir en cuanto a la legislación del tratamiento de los datos personales. Las razones son varias, al ser una ley ágil y con una aplicación territorial determinada teniendo una coherencia con las demás legislaciones (UE). Respecto al desafío de las redes sociales y el consentimiento hay un mejor tratamiento y regulación por parte del reglamento.

Además, el RGPD tiene como prioridad a la persona, brindándole nuevas herramientas y que cuentan con una aplicación efectiva y eficiente, pudiendo ejercer de manera informada y consciente sus derechos en atención al tratamiento de los datos personales. Por último, cuentan con una autoridad encargada de fiscalizar el correcto tratamiento de los datos. Todas estas características son las que estaría careciendo nuestra actual legislación en cuanto a la materia, es urgente modernizar

y hacer frente a los nuevos desafíos, priorizando proteger a la persona por sobre cualquier otra entidad, empresa u organismo público.

4) Situación en Chile:

La Ley N°19.628, también conocida como Ley de datos personales, fue promulgada el 28 de agosto de 1999 titulada "Sobre la Protección de la vida privada" pues en el proyecto original y como su nombre lo indica, se contenían disposiciones relativas a la protección de la vida privada. Sin embargo, durante la tramitación de la ley se suprimieron aspectos generales de la protección de la intimidad, quedando solamente regulada la protección de los datos personales, excluyendo otras formas de intromisión de la vida privada.

Cabe mencionar que el derecho a la intimidad o vida privada no ha sido muy investigado por la Doctrina en Chile y tampoco ha sido muy debatido por el poder Legislativo. Actualmente no existe una ley de protección civil de la vida privada y tampoco existen tipos penales que protejan adecuadamente ésta.

Como lo señala Pablo Viollier en su artículo "El Estado de la Protección de Datos Personales en Chile", *"Existe consenso en la doctrina que la legislación chilena provee un esquema débil para la protección efectiva de los datos personales. Esto se debería entre otras razones, al hecho de que su contenido fue condicionado por ciertos intereses durante la discusión legislativa. Este diagnóstico se ve en el nivel de protección otorgado por la ley, que se caracteriza por ofrecer un marco regulatorio para el mercado de las bases de datos personales, más que por garantizar protección a los derechos de las personas titulares de estos[9]."*

Aquello mencionado en el párrafo anterior se ve claramente reflejado en la Ley citada, pues inmediatamente en su 1° artículo, inciso segundo establece que *"Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos*

[9] VIOLLIER, Pablo. El Estado de la Protección de Datos Personales en Chile. [en línea]: Derechos Digitales. 2017. [fecha de consulta: 4 octubre 2018]. Disponible en: <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf>

fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce". Es decir, el primer derecho consagrado en la ley es el que tienen todas las personas a hacer tratamiento de datos personales y luego, recién a partir del artículo 12° estableció los derechos que tienen los titulares de datos personales.

La Leges Data, en atención al principio de acceso a la información de la persona interesada, estableció un procedimiento judicial para que los afectados en el tratamiento de sus datos personales pudieran resguardar sus derechos. Al no existir una instancia administrativa sino solo un procedimiento judicial, resulta difícil de aplicar pues entre otras razones, se necesita el patrocinio de un abogado. Como ya habíamos adelantado, la normativa no creó un órgano encargado de controlar y ejercer fiscalización al tratamiento de datos personales de registros privados[10]. Es decir, no existe un ente que fiscalice y prevenga las infracciones, pues las personas si ejercen la vía judicial, es porque ya fueron afectadas de alguna manera.

En Chile existe el impulso legislativo-con poca concreción- para adoptar nuevas normativas en cuanto a la protección de los datos. Este impulso se manifiesta en todos los proyectos de ley que tratan de regular esta materia, encontrándose actualmente uno en tramitación para crear la Agencia de Datos, a través de la Reforma Boletín N°11092-07. Estas problemáticas ya habían sido debatidas en algunos países europeos y a partir de la década de 1970 comenzó a legislarse sobre esta materia en el continente europeo. En el caso de Europa podemos apreciar a modo de ejemplo, el Comisario Federal, figura que ejercía fiscalización y regulación de los datos en Alemania; en Suecia se le encomendó a un organismo que se llamaba Datainspektionen y en el caso de España con la Agencia Española de Protección de Datos.

El Boletín N°11092-07, ingresó a la Cámara el 17 de enero de 2017 y se le designó urgencia simple en diciembre de 2017. En marzo de este año se inició la Discusión General del Senado y hasta el mes de julio seguía encontrándose en el Primer

[10] Para el tratamiento que realizan los órganos de la Administración del Estado, el Consejo para para la transparencia, tiene entre sus funciones velar por el adecuado cumplimiento de la ley N° 19.628, establecido en el artículo 33 letra m) de la Ley N° 20.285, sobre acceso a la información pública.

Trámite Constitucional. Esto se debió en parte a que, durante cuatro sesiones ordinarias y sucesivas, entre las fechas del 3 de abril hasta el 3 julio del presente año, se postergaron las indicaciones por parte de los legisladores y se fueron extendiendo los plazos para ser presentadas ante la Cámara, el cual fue presentado el 6 de Julio como el Boletín de Indicaciones respecto al proyecto de ley en cuestión.

Lamentablemente, con fecha 6 de julio del presente año, en el primer trámite constitucional del Senado, se establecieron varias indicaciones que buscaron modificar el proyecto original. Dentro de la más relevante a comentar es la del artículo 30: *"185.- De Su Excelencia el presidente de la República, para reemplazarlo por el siguiente: Artículo 30.- Autoridad de Control. El Consejo para la Transparencia y la Protección de Datos Personales, creado en la ley N° 20.285 sobre Acceso a la Información Pública, será el órgano encargado de velar por el cumplimiento de la normativa relativa al tratamiento de datos personales y su protección, como de todos los derechos consagrados en esta ley."*[11]

Como informó el diario La Tercera, *"Aunque algo se había esbozado, no dejó de sorprender la decisión del Gobierno de cambiar el proyecto de Protección de Datos Personales, eliminando la idea de crear una nueva agencia especial para el tratamiento de la información para dejar en cambio esa labor en el Consejo para la Transparencia […] Ahora el gobierno optó por este esquema que también significa un ahorro de costos, ya que sólo se le otorga un nuevo objetivo a un organismo que ya existe. Aunque desde La Moneda explican que la diferencia presupuestaria no es tanta, sino que implica menor burocracia, pues el CPLT sólo tendría que crear una nueva unidad especializada, se suma un director y se le solicita dedicación exclusiva. "Es un ahorro en eficiencia", acotaron".*[12]

[11] Cámara de Diputados de la República de Chile [en línea]: Proyectos de ley sobre protección de datos personales. [fecha de consulta 26 de noviembre de 2018]. Disponible en: <https://www.camara.cl/pley/pley_detalle.aspx?prmID=11608&prmBoletin=11092-07>

[12] Diario La Tercera. [en línea] "Parlamentarios y privados discrepan por Ley de Datos". 2018. [fecha de consulta: 26 de noviembre de 2018]. Disponible en: <https://www.latercera.com/pulso/noticia/parlamentarios-privados-discrepan-ley-datos/235786/>

En nuestra opinión, creemos que aquel giro en el proyecto N°11092-07 fue lamentable pues ya es tiempo de que nos encontremos a la altura de los estándares internacionales, países que hace décadas cuentan con un organismo especializado y autónomo encargado de fiscalizar y sancionar los incumplimientos de la ley de datos personales. Todo lo contrario, a lo decidido por el Gobierno que le dará aquella facultad a un ente especializado en organismos públicos por lo engorroso que puede ser crear una entidad nueva.

CAPÍTULO 2:

DATOS PERSONALES Y SU NATURALEZA JURÍDICA.

5) Concepto de Datos Personales

La protección de los Datos Personales se encuentra tratado a nivel legal en nuestro país con la ley N° 19.628 y desde la publicación el 16 de junio del presente año de la ley N° 21.096, y tiene consagración constitucional. Aquella ley, incorporó a la Constitución Política de la República, en el numeral 4° del artículo 19° sobre la protección a la vida privada y la intimidad, la protección de los datos personales, mencionando además que el tratamiento y protección de ellos se efectuará en la forma y condiciones que determine la ley. Con la última frase, se remitió entre otras leyes, a la N° 19.628, la cual como hemos ido adelantando, no es del todo eficiente para cumplir con el mandato constitucional.

Los Datos Personales están definidos en la ley 19.628 en su artículo 2 letra f) y "*son los relativos a cualquier información concerniente a personas naturales identificadas o identificables."* La ley establece que esta ley solo será aplicable cuando la persona titular de los datos personales sea una persona Natural. Lo cual nos parece motivo de critica que ahondaremos en el capítulo correspondiente pues las personas jurídicas también poseen datos que pueden ser objetos de tratamiento, viéndose perjudicadas.

Entendemos por Dato Personal entonces, información relevante como el Nombre, Domicilio, Número de Identificación Personal (RUT), Número de Teléfono, Número de la Tarjeta de Crédito y de las Cuentas Bancarias, Patente del Auto, Afiliación a AFP, a Isapre, entre otros. Hoy en día en el sector de las Telecomunicaciones, en especial con el avance tecnológico y la masificación del acceso a internet y con toda la información que ellos almacenan, los datos personales se han ido ampliando abarcando entre otras cosas, por ejemplo, la Dirección de Correo Electrónico, todo

lo contenido en el Perfil de Facebook, Instagram, Twitter que incluya información relativa a la persona natural, identificada o identificable.

Otros conceptos que definiremos a continuación, pues usaremos a lo largo de este trabajo son:

Responsable del registro o banco de datos, definido en la ley N° 19.628 en el artículo 2, letra n), como *"la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento con el tratamiento de los datos de carácter personal".*

Entendiéndose por tratamiento de datos, según el artículo 2 letra o, de la misma ley, *"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".*

Una de las críticas que hacemos a esta ley, es que solo definió al responsable del banco de datos, pero no al tercero que solicita información. Serán terceros y no responsable de la base de datos, aquellos que les solicitan a los responsables de la base de dato, comunicación sobre datos, sin que efectúen un tratamiento que implique una nueva base de datos. Es decir, el artículo 5° se refiere escuetamente a ellos, al señalar que, en caso de requerir transmisión de datos personales por medio de una red electrónica, quien hace el tratamiento (es decir el tercero) se hace responsable por ello, debiendo respetar la finalidad que motivó la transmisión[13].

6) Clasificación de los Datos Personales:

Para explicar y comentar ciertos aspectos de los datos personales en Chile, vamos a clasificarlos de diferentes maneras.

[13] ALVARADO ÁLVAREZ, Francisco. Internet y las fuentes de acceso público a datos personales. (Licenciado en Ciencias Jurídicas). Santiago, Chile: Universidad de Chile, escuela de Derecho. 2013. 194 pág.

6.1) Directos e Indirectos:

Los Datos Directos, son aquellos que se han conseguido a través de la voluntad de su titular quien ha entregado información respecto de su persona con su expreso consentimiento. A contrario sensu, los Datos Indirectos, son los que han sido recolectados desde otros bancos de datos que han hecho tratamiento de estos.

Cabe señalar que el artículo 5 de la ley señalada, permite que el responsable del banco de datos personales transmita[14] aquellos datos a un tercero cumpliendo los requisitos de cautela de los derechos de los titulares y que la transmisión guarde relación con las tareas y finalidades de los organismos participantes, de manera que el tercero receptor de los datos solo pueda utilizarlos para los fines que motivaron la transmisión.

Este tema de la comunicación o transmisión de datos a terceros, que genera datos personales indirectos de manera fácil en relación con otros países que lo restringen, lo analizaremos en el capítulo sobre las críticas a la Ley N° 19.628. Adelantamos otra crítica importante, al artículo 5 de la ley citada; la cual no hace mención de la transferencia internacional de datos, cuestión que la transforma en una ley anacrónica que no cuenta con los rangos internacionales, al no establecer la protección transfronteriza de datos.

6.2) Públicos y Privados:

Los Datos Públicos son aquellos que se encuentran disponibles para cualquier interesado por encontrarse en registros o lugares de fácil acceso al público, por ejemplo, resultados de censo, repertorios de jurisprudencia y directorios de teléfono. Tienen amplia crítica como explicaremos en otro capítulo, pues este tipo de datos recolectados de fuentes accesibles al público son una excepción al consentimiento expreso del titular de los datos para que entre otras cosas sus datos sean

[14] Artículo 2 letra c, ley N° 19.628 señala “Comunicación o transmisión de datos, dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas”.

recolectados, tratados, transmitidos o excluidos del principio de finalidad[15]. Respecto de las reglas para la transmisión de datos[16] por parte del responsable de la base a terceros, no se aplicarán si son transmisiones que recaigan sobre datos personales accesibles al público en general.

Por otro lado, los Datos Privados, son aquellos que no se encuentran disponibles al público pero que han sido obtenidos de otras maneras que la ley permite.

La Ley en su Artículo 4° señala que solo puede efectuarse el tratamiento de datos personales cuando la ley lo autorice o el titular consienta expresamente en ello. Aquella regla general es ilusoria pues en los siguientes incisos del mismo artículo, señala una excepción, que dispone que no requiere autorización el tratamiento de datos personales que provengan o se recolecten de: fuentes accesibles al público, cuando sean de Carácter Económico, Financiero, Bancario o Comercial, se contenga en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Los que se dedican a lucrar con el tratamiento de datos personales, se suelen excusar con que tratan datos personales públicos, pero aquello es ambiguo pues no existe claridad sobre qué es público, ya que la definición de fuentes accesibles al público[17] no señala taxativamente cuales son estas fuentes, siendo un tema extremadamente delicado pues no están establecidos legalmente los límites de nuestra esfera intima versus lo que pertenece a nuestra esfera pública o social,

[15] Artículo 9, inciso primero, Ley 18.628 señala que "Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público".
[16] Artículo 5, inciso primero Ley 18.628 señala que "El responsable del registro o banco de datos personales podrá establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes".
[17] Artículo 2, letra i) "Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes".

dando cabida a vulneraciones. Diferente es lo que ocurre en España donde existe un catálogo taxativo sobre cuáles son las fuentes accesibles al público.

6.3) Sensibles y No Sensibles:

Los Datos Sensibles se definen en el Artículo 2°, letra G de la ley N° 19.628 como: "*aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual*."

Los Datos Sensibles tienen un tratamiento especial en atención a su contenido y se encuentran regulados brindándoles mayor protección que a los datos no sensibles, los cuales operan por exclusión y tienen menor grado de protección. Estos fueron tratados por primera vez en el Convenio 108 de 1981 efectuado por el Consejo de Europa para la protección de la vida privada de los individuos con respecto a los bancos electrónicos privados y públicos y no podrán ser tratados a menos que una 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.[18]

Subsiguientemente en la definición en el artículo 2 letra g) de la ley 19.628, a través de un listado genérico se señalan ejemplos de datos sensibles: *"hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual".* Ejemplos de datos sensibles "modernos" son los datos biométricos y datos relativos al perfil biológico humano.

Todos los datos que no correspondan a la categoría anterior son considerados como No Sensibles y al operar por exclusión tienen un tratamiento menos protegido y estos podrían ser el nombre, RUT y llegando incluso al número de teléfono. Se

[18] Artículo 10 ley N° 18.728.

discute si el domicilio se configura como Dato Sensible y debe ser protegido como tal, nosotros creemos que si lo es.

6.4) Tratamiento por Bancos de Datos Personales a cargo de Organismos Públicos y por Bancos de datos a cargo de Privados.

El artículo 22 de la ley establece que el Servicio de Registro Civil e Identificación, deberá llevar un registro de los bancos de datos personales a cargo de organismos públicos, estando establecidas las normas de aplicación para aquello en el Reglamento del Registro de bancos de datos personales a cargo de organismos públicos contenido en el Decreto Supremo N° 779, de 11 de noviembre de 2000. Pese a lo anterior, el Servicio de Registro Civil e Identificación carece de facultades legales para obligar y sancionar el incumplimiento de estos organismos públicos, quedando a disposición de ellos cumplir con la ley.

Respecto de las bases de datos personales a cargo de privados, no existe un Registro general donde deban inscribirse aquellas bases, impidiendo a los ciudadanos en la práctica conocer a las entidades que procesan y tratan sus antecedentes, no pudiendo ejercer de esta manera los derechos que les confiere la ley a los titulares de datos afectados.

7) Naturaleza Jurídica y Bien Jurídico Protegido

Los datos personales tienen la naturaleza jurídica de garantía constitucional, al protegerse aquellos y ser parte del derecho inherente de todas las personas a tener intimidad y vida privada, del Articulo 19 Nº4 de nuestra Carta Magna. Anterior a la publicación de la ley N° 21.096, la doctrina igualmente indicaba que se consideraba incorporado como un aspecto de la privacidad.

Con la ley N° 21.096 que agregó la protección de los datos personales al artículo 19 n°4 de la Constitución Política de la República, aquel artículo quedó estipulado de la siguiente manera:

“La constitución asegura a todas las personas:

4° El respeto y protección a la vida privada y a la honra de la persona y su familia, 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;"

Al ser parte de una garantía constitucional, quien sea víctima de un tratamiento inconstitucional de sus datos personales, puede interponer una Acción de Protección del artículo 20° de la Constitución Política de Chile. Como dato relevante señalamos que algunos recursos de protección respecto de datos personales fundados en la vulneración de la intimidad y vida privada han sido rechazados en atención al principio de especialidad, pues la ley N° 19.628 establece un procedimiento judicial para aquello. Aquello claramente es respecto a acciones anteriores a su protección constitucional expresa, a seis meses de su consagración constitucional, no existe claridad sobre los cambios e incidencia de aquello.

A su vez podemos señalar que los atributos de la personalidad también forman parte de los datos personales.

CAPÍTULO 3:

REGULACIÓN DE LA LEY 19.628 Y SU APLICACIÓN.

8) Derechos del Titular de los Datos Personales:

El Titulo II de la Ley N° 19.628, llamado de "*los derechos de los titulares de los datos",* en su Artículo 12° dispone una serie de derechos comunes para los titulares de los datos, señalando los siguientes:

b) El Derecho de **A**cceso.
c) El Derecho de **R**ectificación o Modificación.
d) El Derecho de **C**ancelación.
e) El Derecho de **O**posición o Bloqueo.

A continuación, pasaremos a explicar en qué consiste cada Derecho que goza el Titular de datos personales, a los cuales se les ha denominado por la doctrina como los "Derechos ARCO" debido a sus iniciales.

a) Derecho de Acceso, permite a los titulares de los datos personales acceder al registro o base de datos ya sea público o privado, para acceder a la información de sus propios datos, su procedencia, el objetivo de estos y la individualización de los terceros a los cuales son cedidos. [19]

b) Derecho de Rectificación o Modificación, consiste en la facultad que tiene el titular de los datos para requerir que se modifiquen estos en el caso que sean erróneos, inexactos, equívocos o incompletos y así se acredite.

c) Derecho de Cancelación o Eliminación, señala que el titular de los datos personales tiene el derecho a exigir que se eliminen los datos en caso de

[19] Artículo 12, inciso primero de la Ley N° 19.628.

que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos, sin perjuicio de las excepciones que existan en la ley.

La ley dispone a través de mandato expreso, las situaciones en que un dato se encuentre *caduco*:
i) el que ha perdido actualidad por disposición de la ley.
ii) el que ha perdido actualidad por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia.
iii) si no hubiera norma expresa, por el cambio de los hechos o circunstancias que consigna.

d) El Derecho de Oposición o Bloqueo, corresponde a la facultad del titular de datos almacenados para solicitar la suspensión temporal de las operaciones de tratamiento cuando la exactitud de los datos no pueda ser establecida, o su vigencia sea dudosa y respecto de los cuales no corresponda la cancelación.

Los Derechos mencionados anteriormente tienen como característica común que tienen que ser proporcionados de manera completamente gratuita a su titular.

8.1) Límites al ejercicio de estos derechos.

El artículo 13° de la ley de datos personales, señala que por regla general los derechos anteriormente mencionados no pueden ser limitados por ningún acto o convención alguna. Pero instaura como excepciones en el artículo 15°, que no se podrá acceder al derecho cuando impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido (Por ejemplo, si un contribuyente solicita los datos de carácter tributario del año en curso al Servicio de Impuestos Internos), o afecte la reserva o secretos establecidos en disposiciones legales o reglamentarias (Por ejemplo, si se trata de datos personales que constan en expedientes judiciales que revisten el carácter de secreto según la ley, como en el caso de las adopciones o juicios de menores), o afecta la seguridad de la nación o el interés nacional. El último inciso del artículo señala que tampoco podrá pedirse

la modificación, cancelación o bloqueo de datos de registros o bancos de datos creados por mandato legal, salvo que la propia ley lo autorice. No se hace extensiva al derecho de información[20].

8.2) Mecanismos para hacer valer los derechos de los Titulares de datos:

8.2.1) Habeas Data:

La vía principal para ejercer los derechos en Chile es el Habeas Data que es una acción cautelar de rango legal[21], derivada del Habeas Corpus, que en las modernas sociedades de la información permite a los titulares de los datos personales y patrimoniales "autodeterminar" el uso que se haga de sus antecedentes cuando ellos son recopilados, registrados y cruzados computacionalmente. El Habeas Data actúa sobre la autodeterminación informativa, ya sea que lo haga de manera judicial o extrajudicial el titular de los datos.

Las causales de procedencia del Habeas data, están contenidas en el Artículo 16° de la ley de datos personales. El sujeto activo de tal acción es el titular de los datos personales y debe dirigirse contra el responsable del banco de datos sea organismo público o privado que denegó algún derecho o ha realizado tratamiento indebido de aquellos.

8.2.1.1) Procedimiento de Habeas Data:

El artículo 16° además de contener las causales de procedencia, establece dos procedimientos diferentes dependiendo de la gravedad del asunto. En términos generales señalaremos los dos procedimientos que contiene la ley, que clasificaremos como general y especial, para luego analizar y realizar observaciones a sus falencias.

[20] Derechos del Titular de Datos y Habeas data en la ley 19.628. [en línea]. Santiago, CHILE. 2003. Revista Chilena de Derecho Informático, Centro de Estudios Informáticos de la Facultad de Derecho de la Universidad de Chile. [fecha de consulta: 4 octubre 2018] Disponible en: <http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_simple/0,1493,SCID%253D14180%2526ISID%253D292%2526PRT%253D14178,00.html>

[21] En Chile, pues hay muchos países que reformaron su Constitución y lo incorporaron, como Argentina, Brasil, Colombia, Perú, Paraguay y Venezuela.

8.2.1.2) Procedimiento general**:**

Establecido en el segundo inciso del artículo 16° de la Ley N° 19.628, procede cuando el responsable del banco de datos no se pronuncie sobre un requerimiento dentro del plazo de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional o se cometiera infracción a lo dispuesto en los artículos 17° y 18° de la misma ley[22], siendo competente para conocer de la acción el Juez de Letras en lo Civil correspondiente al domicilio del responsable de la base de datos. El mismo artículo señala los requisitos que debe contener la reclamación (señalar claramente la infracción cometida, los hechos que la configuran acompañando los medios de prueba que los acrediten si así fuera el caso), estableciendo que aquel requerimiento se notifica por cédula al responsable del banco de datos. Este tendrá plazo para contestar dentro de 5 días hábiles desde la notificación donde debe adjuntar los medios de prueba que acrediten los hechos en los que se funda (Art. 16 letra b).

En el caso de no disponer de medios de prueba al contestar la demanda, el responsable deberá informarlo y el tribunal fijará una audiencia para dentro del quinto día hábil para ofrecer y rendir prueba.

Una vez que se vence el plazo fijado para la audiencia de prueba o se vence el plazo para contestar, se hayan presentado pruebas o no, el juez dictará sentencia definitiva dentro de tercero día. Esta última es apelable en ambos efectos dentro del plazo de 5 días hábiles desde la notificación del recurrente. Se le da preferencia a la vista del recurso viéndose en un principio en cuenta.

[22] El artículo 17, inciso primero, primera parte de la ley N° 19.628, es muy importante pues fue reformado con la Ley N°20.725 y señala, "Los responsables de los registros o bancos de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas consten en letras de cambio y pagarés protestados; cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales".

Por otro lado, los bancos de datos a cargo de organismos y entidades privados no tienen la obligación de contar en un registro, ni tampoco existe un organismo que se encargue del control y fiscalización de estos datos. En la práctica esto tiene un efecto muy nocivo pues dificulta a las personas dirigirse contra el responsable del banco de datos para ejercer sus derechos, pues como mencionamos el Juez de Letras en lo Civil competente para conocer de la acción, es el del domicilio del responsable de la base de datos.

8.2.1.3) Procedimiento especial:

Regulado en los incisos tercero y cuarto del mismo artículo 16°, establece que, si la causal por la cual se negase el pleno ejercicio de los derechos de los titulares de datos fuese la seguridad de la nación o el interés nacional, el *Habeas Data* deberá ser deducido directamente ante la Corte Suprema. El sujeto pasivo de este procedimiento son solo los organismos públicos[23].

Los requisitos de lo que debe contener la reclamación y su forma de notificación son de la misma manera que en el procedimiento general. La corte Suprema luego de recibir la reclamación solicitará de la manera que considere más rápida, informe de la autoridad de que se trate fijándole plazo para el efecto, transcurrido el cual resolverá en cuenta la controversia. Si se recibe prueba, esta se mantendrá en reservado. La reclamación se verá en cuenta, pero de la misma manera que en el procedimiento general respecto de la apelación, se podrá ordenar traer los autos en relación para oír a los abogados, si lo estima conveniente o se le solicita con fundamento plausible, caso en el cual la causa se agregará extraordinariamente a la tabla de la respectiva sala.

8.2.1.4) Sanciones:

[23] Debido a que son los únicos que tienen la facultad de oponerse en atención a la causal de la seguridad de la Nación o el interés Nacional. Los organismos públicos se encuentran definidos por la Ley N° 19.628 en el artículo 2, letra K) "Organismos públicos, las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1° de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado".

El mismo artículo 16° en sus incisos quinto y sexto señala que en caso de dictarse sentencia definitiva ejecutoriada acogiendo la reclamación, ésta fijará un plazo prudencial para dar cumplimiento a lo resuelto, pudiendo además establecer las siguientes sanciones, que son extremadamente bajas, para los responsables de bases de datos:

- Multa de diez a cincuenta unidades tributarias mensuales[24] en el caso que se infrinja lo dispuesto en los artículos 17° y 18°, es decir las normas especiales respecto a los datos económicos, financieros, bancarios y comerciales.

- Y multa de una a diez unidades tributarias mensuales en todos los otros casos.

En el caso de la falta de entrega oportuna de la información o el retardo en efectuar la modificación, el juez podrá aplicar una multa de dos a cincuenta unidades tributarias mensuales y si el responsable de datos fuere un organismo público el tribunal podrá sancionar al jefe del servicio con la suspensión de su cargo, por un lapso de cinco a quince días.

8.2.1.5) Responsabilidad:

Además de la sanción mencionada anteriormente, el Artículo 23° agrega la "Responsabilidad del banco de datos personales" por los daños patrimoniales y morales que fuesen causados por el tratamiento indebido de los datos aludidos, pudiendo fijar el juez el monto de la indemnización de perjuicios de ser requerida por el afectado que lo solicite al tribunal. La Acción de Indemnización de perjuicios puede conocerse en forma conjunta con el Habeas Data, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil.

[24]Aquellos montos fueron modificados con la Ley N° 19.812 de 13 de junio de 2002, pues anterior a eso era de una a diez unidades tributarias mensuales.

Respecto al sistema de Responsabilidad, la Jurisprudencia[25] ha señalado que la ley N° 19.628 se refiere a un sistema de responsabilidad común del Código Civil, en nuestra opinión resulta perjudicial, pues al encontrarse amenazados derechos fundamentales tan importantes como la privacidad y la vida privada, a manos de Terceros y Responsables de bancos de datos que se dedican en su mayoría a lucrar con ellos, la responsabilidad debiese ser objetiva y no un sistema de responsabilidad por culpa, pues aquello sumado a que las sanciones pecuniarias por infringir la ley son irrisoriamente bajas, no existe ningún incentivo para terminar con aquellas malas prácticas. Sumado a lo anterior, no existe una autoridad de control que supervise y fiscalice preventivamente el cumplimiento de la normativa.

8.2.2) Vía Judicial Indirecta (Acción de Protección):

A la persona natural titular de datos a la cual, con el tratamiento de sus datos personales, se vea privado, perturbado o amenazado en el legítimo ejercicio de sus derechos y garantías constitucionales señaladas en el artículo 20 de la Constitución Política de la República, podrá interponer una Acción de Protección.

No solo la garantía del artículo 19 n°4 de la Constitución Política de la República, que señala “El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales”[26], puede verse transgredida por un tratamiento indebido de datos personales, sino también por ejemplo el derecho a la libertad de trabajo y su protección[27], lo cual legitima para poder interponer una Acción de Protección con el fin de solicitarle a la Ilustrísima Corte de Apelaciones que tome medidas para que ponga fin a la privación, perturbación o amenaza de ese derecho.

---

[25] Fallo Corte Suprema, ROL 6968-2010, caratulado Banco Santander Banefe con Lobos Quijanes Ángel”, en autos sobre Indemnización de perjuicios.

[26] Ley N° 21.096 publicada el 16 junio de 2018, Artículo único.- Agregase, en el numeral 4° del artículo 19 de la Constitución Política de la República, a continuación de la expresión "y su familia", lo siguiente: ", 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".

[27] Consagrado en el artículo 19 N° 16 de la Constitución Política de la República.

Al cruzarse computacionalmente información entre bases de datos con información sobre una persona natural, se pueden elaboran perfiles que atentan contra los derechos y garantías de las personas, aquello creemos, es muy grave.

8.2.2.1) Caso sitio web: http://datos.24x7.cl.[28]

Mencionaremos la acción de protección que presentó el 2015 la organización Datos protegidos ante la Corte de Apelaciones de Santiago, donde solicitó que ordenara dar de baja al sitio por la vulneración del derecho a la privacidad. Aquello fue pues el RUT es un dato personal necesario para la vida pública, pero es una verdadera clave de acceso a otros datos personales que pueden o no ser sensibles.

Aquella página que actualmente se encuentra deshabilitada, era una de las tantas que actualmente se encuentran disponibles y que nos ofrecen datos personales de distintos individuos. Generalmente se puede encontrar el nombre completo, RUT y Domicilio. La defensa señaló que la información había sido ofrecida por el mismo Estado a través de la página del SERVEL (Servicio Electoral) en donde se encontraban archivos PDF con listados de la información que ellos ofrecían en sus sitios. Fue por eso por lo que la Corte no acogió la Acción de protección y la Excelentísima Corte Suprema el año 2016 ratificó el fallo de fecha 3 de junio del año 2015, haciendo énfasis en que la información fue obtenida de una fuente de acceso público y que no se logró demostrar que haya sido transgredido una garantía a las personas, desestimando que a través de la publicación de los tratamientos de datos se haya afectado la vida privada y la intimidad de los recurrentes. Asimismo, los datos que entregaba la página no fueron considerados sensibles, siendo a nuestro juicio discutible respecto del domicilio. Actualmente la página no se encuentra en funcionamiento, pero existe una docena de sitios parecidos dedicados al mismo negocio.

[28] Noticia disponible en <https://datosprotegidos.org/24x7-somos-personas-no-codigos/>

9) Comparación proyecto original con la ley publicada.

Al momento de presentarse el proyecto en el Congreso de la actual ley de datos personales en Chile, nos encontrábamos muy atrasados con respecto a otros países. El proyecto de ley fue inspirado por la normativa de España, Francia, Reino Unido, Noruega, legislaciones que datan entre las décadas de los años 70´ y 80´[29]. A medida que el proyecto se tramitaba, fue tomando relevancia el texto de La Ley Orgánica 5/1992 sobre regulación del tratamiento automatizado de los datos de carácter personal de España, pudiendo llegar a considerarse la ley N° 19.628 tributaria de esta[30].

Por lo anterior fue que la moción aprobada por el Senado fue muy completa al intentar proteger la vida privada en su totalidad, pero luego de 6 años de tramitación[31], el proyecto original terminó reducido a una ley que protegió específicamente los datos personales y de manera insuficiente.

A continuación, realizaremos una breve comparación entre el proyecto de ley original y el texto legal finalmente aprobado y promulgado. Primero señalaremos aspectos que se contenían en el proyecto original y que luego se omitieron y seguidamente mencionaremos aspectos importantes que durante la tramitación del proyecto se agregaron al texto finalmente aprobado.

9.1) Bien jurídico protegido:

Al analizar el proyecto de ley original “sobre protección civil de la vida privada” del año 1993 en comparación con la ley N° 19.628, podemos apreciar objetos de protección distintos.

[29] Ley orgánica N° 1, del 05 de mayo de 1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen de España; Ley 78-17, de 06 de enero de 1978, sobre informática, ficheros y libertades de Francia; Ley del 12 de julio de 1984, sobre protección de datos del Reino Unido, Ley 48, de 09 de junio de 1978, sobre registros de datos personales de Noruega.

[30] VIOLLIER, Pablo. El Estado de la Protección de Datos Personales en Chile. [en línea]: Derechos Digitales. 2017. [fecha de consulta: 4 octubre 2018]. Disponible en: <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf>

[31] Proyecto de ley fue presentado el 05 de enero de 1993.

El proyecto de ley contemplaba la protección de la vida privada de las personas en su totalidad según se desprende de los artículos 1° al 8° del proyecto original, a contrario sensu de la ley publicada, que no trató en profundidad aquella protección, quedando normado y como objeto de protección, solo el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares. Esto explica por qué la ley se llamó “sobre protección de la vida privada” y solamente se refirió a la protección de los datos personales.

9.2) Actos ilegítimos que afecten la vida privada:

El proyecto de ley en sus artículos 14° al 19° señalaba ciertos actos que se consideraban ilegítimos para la vida privada como, las escuchas, filmación, la divulgación o revelación de información, utilización del nombre, el acoso reiterado ilegitimo mediante llamadas, correspondencia y el acecho del hogar. Finalmente, la ley aprobada no contempló un listado de intromisiones a la vida privada que fueran catalogadas de legitimas e ilegitimas.

9.3) Derecho al titular de los datos personales a acceder a la información sobre aquellos:

El proyecto de ley en su Artículo 11° señalaba el derecho a la información del titular sobre los datos tratados, conocidos como “Habeas Data”, a posteriori en el texto final, en su Artículo 16° se estableció un procedimiento especial más complejo haciendo de esta manera más engorroso el derecho a la información cuando no fuera debidamente respondida la solicitud dentro de dos días hábiles.

9.4) Tratamiento de datos por un organismo público y uno privado:

El proyecto de ley no contemplaba la distinción entre tratamiento de datos por un organismo público y por un ente privado. Finalmente, la ley aprobada hizo una distinción importante entre estos dos estableciendo el título IV “Del tratamiento de datos por los organismos públicos”, en los artículos 20 a 22. Una norma importante de comentar es la del artículo 22 que dispone que los bancos de datos públicos deben inscribirse en un Registro de bancos de datos personales a cargo del

Registro Civil, al cual no le dieron facultades fiscalizadoras ni sancionatorias para hacer cumplir la norma.

9.5) Definiciones de algunos conceptos técnicos:

El proyecto de ley no contemplaba definiciones de los conceptos relevantes para la aplicación de esta misma. Por otra parte, la ley N° 19.628 definió en su Artículo segundo, desde la letra a) a la o) ciertos conceptos para mejor comprensión y aplicación de la materia.

Stricte dictu el Artículo 2° define; almacenamiento, bloqueo, comunicación o transmisión de datos, dato caduco, dato estadístico, datos de carácter personal, datos sensibles, eliminación o cancelación de datos, fuentes accesibles al público, modificación de datos, organismos públicos, procedimiento de disociación de datos, registro de bancos de datos, responsable del registro y titular de los datos.

9.6) Procedimiento de transmisión automatizada de datos:

El proyecto de ley no lo abordaba, pero la norma final trató esta materia en su Artículo 5°, señalando que el responsable de los bancos de datos personales podrá establecer un procedimiento automatizado de transmisión siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las finalidades de los organismos participantes, señalando además los requisitos que se deben cumplir para poder efectuarlos.

9.7) Deber de Secreto de personas que trabajan en el tratamiento de datos personales:

El proyecto de ley no señalaba el deber de secreto ni hacía mención alguna a aquel concepto. A contrario sensu la ley en su Artículo 7°, señala que las personas que trabajan en el tratamiento de datos personales, que no hayan sido recolectadas de una fuente accesible al público, están obligadas a guardar secreto sobre estos mismos.

Pese a que la ley incorporó aspectos importantes que el proyecto original no había considerado, se excluyeron todas las disposiciones relativas a la protección de la

vida privada, aprobando finalmente una ley sucinta de solo 24 artículos, con excepciones muy amplias sobre todo respecto del tratamiento de los datos personales de fuentes accesibles al público. A continuación, mencionaremos las modificaciones que se han hecho a la ley N° 19.628 en atención a mejorar los estándares de protección de datos personales, buscando terminar con los abusos y su comercialización.

10) Modificaciones a la Ley N° 19.628.

La ley N° 19.628 ha sido objeto de varias modificaciones y como señala VIOLLIER *"La mayoría de están han tenido por objeto remediar ciertas situaciones de discriminación o vulneración que sufrían las personas debido al tráfico de sus datos personales por parte de empresas. Sin embargo, ninguna de estas modificaciones supuso una reforma integral a la ley, ni se abocó a suplir de manera general algunas de sus falencias estructurales. Es por esto que pueden ser catalogadas como "leyes parche"".*[32]

10.1) Ley N° 19.812 "Modifica la ley N° 19.628, sobre protección de la vida privada", publicada el 13 de junio de 2002, consiste en 2 artículos y 3 transitorios:

El artículo 1 N° 1, modificó el monto de la multa señalada en el inciso 5° del artículo 16° de la Leges Data, aumentándola de 10 a 50 Unidades Tributarias Mensuales, cuando se cometiera una infracción a los artículos 17° y 18°.

Como ya lo habíamos comentado en un capítulo precedente, hasta antes de esta ley la multa era de 1 a 10 Unidades Tributarias Mensuales y a nuestro parecer el aumento de la multa fue infructífero pues siguió sin ser un incentivo para respetar la norma. Es una multa muy baja, de máximo 2.417.650 millones de pesos chilenos[33].

[32] VIOLLIER, Pablo. El Estado de la Protección de Datos Personales en Chile. [en línea]: Derechos Digitales. 2017. [fecha de consulta: 4 octubre 2018]. Disponible en: <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf>

[33] Según precio UTM de diciembre de 2018, disponible en Servicio de Impuestos Internos.

El artículo 1° N°2 agregó en el inciso primero del artículo 17, la siguiente frase “Se exceptúa la información relacionada con los créditos concedidos por el Instituto Nacional de Desarrollo Agropecuario a sus usuarios”.

El artículo 1 N° 3, agregó al artículo 17 de la Leges Data, que “no podrá comunicarse la información relacionada con las deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas”.

En el artículo 1 N° 4, se incorporó al artículo 18 de la Leges Data, que bajo ningún caso se podrán comunicar los datos de la información financiera del artículo 17 que se relacionen con una persona luego de transcurrido cinco años desde que la obligación se hizo exigible. Agregando además que no se podrán comunicar los datos relativos a dicha obligación después de haber sido pagada o extinguida por otro modo legal. De igual forma se comunicará a los Tribunales de Justicia la información que requieran con motivos de juicios pendientes.

En el artículo 2, esta ley introdujo al artículo 2° del Código del Trabajo, un nuevo inciso que establece el derecho que tiene el trabajador a que su empleador no pueda condicionar la contratación a la ausencias de obligaciones de carácter económico, financiero, bancario o comercial que conforme a la ley, puedan ser comunicadas por los responsables de registros o bancos de datos personales, ni exigir para dicho fin declaración ni certificado alguno, exceptuándose los trabajadores con labores gerenciales, de representación, administrativas y los que tengan a su cargo la recaudación, administración o custodia de fondos o valores de cualquier naturaleza.

El objetivo buscado por este nuevo inciso en el artículo 2° del Código del Trabajo era erradicar la discriminación de solicitar a los postulantes a un puesto de trabajo su historial financiero condicionando la contratación a no contar con deudas pendientes lo que en la actualidad no se respeta ya que se sigue ejerciendo esta práctica por la falta de un procedimiento y sanciones que lo hagan efectivo.

10.2) Ley 20.463 “Modifica ley N° 19.628, suspendiendo por el plazo que indica la información comercial de las personas cesantes”, publicada el 25 de octubre de 2010:

En su artículo único introduce al artículo 17 de la Leges Data los incisos tercero, cuarto, quinto, sexto, séptimo y octavos, los cuales en términos generales establecen la prohibición a los administradores de datos personales de carácter financiero, económico, bancario y comercial de hacer tratamiento de deudas de personas naturales producidas en el período de cesantía, en especial los protestos y morosidades que afecte al deudor, estableciendo además los pasos a seguir para el bloqueo de datos pues si el individuo no se encuentra incorporado a un seguro de cesantía, él mismo es el encargado de certificar su cesantía ante el Boletín de Informaciones Comerciales acompañando ciertos documentos.

Esta reforma tampoco significó un gran cambio pues solo se refiere a deudas contraídas dentro del período de cesantía y no obligaciones anteriores que no se pudieron cumplir por encontrarse el individuo posteriormente cesante. Además, establece un sistema engorroso para que aquellos que no estén adscritos a un seguro de Cesantía deban realizar el trámite por ellos mismos, para los efectos de impetrar el derecho por tres meses renovable hasta por una sola vez, lo cual asimismo nos parece un período de tiempo insuficiente. Hay personas que no pueden pagar una obligación y eso los perjudica de por vida.

10.3) Ley N° 20.575 publicada el 14 de febrero de 2012, “Establece el principio de finalidad en el tratamiento de datos personales”, publicada 17 de febrero de 2012, más conocida como “Ley DICOM”:

La Ley cuenta con 8 artículos y 2 transitorios. Los artículos 7° y 8° modifican la ley N° 19.628 y los otros primeros son una ley independiente. Su objetivo fue evitar los abusos en el tratamiento de los datos personales de carácter económico, financiero, bancario y comercial por parte de diferentes entidades. Los principales cambios que incorpora esta ley son:

En su primer artículo, establece el principio de finalidad, que consiste en que el tratamiento de los personales de carácter económico, financiero, bancario y comercial será exclusivamente para la evaluación del riesgo comercial y para el proceso de crédito. En el mismo artículo 1°, inciso tercero, prohíbe exigir la comunicación de los datos económicos, financieros, bancario y comercial para tramites de selección de personal, admisión preescolar, escolar o de educación superior, atención médica de urgencia o postulación a un cargo público.

En su artículo 3°, inciso segundo, señala que se faculta al titular de los datos para solicitar gratuitamente a los distribuidores, cada cuatro meses, la información del registro de acceso y entrega de sus datos personales, en el cual se señale el nombre de quienes los han requerido, el motivo, la fecha y la hora de la solicitud.

Prohíbe comunicar la información relacionada con deudas repactadas, renegociadas o novadas, o cuando éstas se encuentren con alguna modalidad pendiente. Asimismo, prohíbe comunicar información sobre deudas contenidas por el uso de autopistas (ya se encontraba prohibido comunicar deudas por deudas de luz, agua, gas).

Introduce mecanismo destinados a facilitar el ejercicio de los derechos de los titulares:

> i) Se invierte la carga de la prueba, estableciendo la obligación del distribuidor o el responsable de los registros o bancos de datos de probar ante el juez que dio cumplimiento a las normas que rigen el tratamiento y comunicación de datos.
>
> ii) Se establece la obligación de los distribuidores de designar una persona natural encargada del tratamiento de datos, frente a la cual los titulares de datos puedan hacer efectivos los derechos reconocidos en la ley, sin perjuicio de su facultad de iniciar las acciones legales que esta misma reconoce.[34]

[34] Biblioteca del Congreso Nacional de Chile [en línea] "Guía Legal sobre Ley Dicom". 2012. [fecha de consulta: 2 de octubre del 2018]. Disponible en <http://www.bcn.cl/leyfacil/recurso/ley-dicom>

El espíritu de esta ley era resguardar los derechos de los consumidores pese a tener obligaciones pendientes, pues existir en el boletín comercial les cierra las puertas a las personas mucho más allá de pedir préstamos y créditos con el banco. Su objetivo era evitar el abuso y lucro en los tratamientos de datos personales por distintas entidades. En marzo de 2012 don Felipe Harboe, diputado en esa época, denunció ante el SERNAC que la empresa EQUIFAX se encontraba vendiendo datos personales con la entrega de antecedentes comerciales a universidades y empresas pese a que la presente ley lo prohíbe, *"Según el parlamentario, tras fiscalizar el funcionamiento e implementación de la nueva ley, se pudo conocer que la empresa Equifax dispuso un sistema de compra de antecedentes comerciales por internet, en el que sólo se exige el Rut y el código verificador de la persona a consultar*"[35].

10.4) Ley 20.521, "modifica la ley N° 19.628, sobre protección de datos de carácter personal para garantizar que la información entregada a través de predictores de riesgo sea exacta, actualizada y veraz", publicada el 23 de julio de 2011.

Esta ley en su artículo único prohíbe la realización de evaluación de riesgo comercial que no esté basado únicamente en información objetiva relativa a las morosidades o protestos de las personas naturales o jurídicas de las cuales se informa. Se establece como sanción a la infracción de lo mencionado anteriormente, la eliminación inmediata de dicha información y da lugar a la indemnización de perjuicios que corresponda.

Como señala VIOLLIER, esta ley es muy acotada pues al tener un solo artículo, es excesivamente breve y no define lo que es *"información objetiva",* reduciendo

[35] Emol [en línea]: "Denuncian nueva infracción de Equifax a días de la entrada en vigencia de "Ley Dicom". 2012 [fecha de consulta: 3 octubre de 2018] disponible en: <https://www.emol.com/noticias/economia/2012/03/02/528908/denuncian-nueva-infraccion-de-equifax-a-dias-de-la-entrada-en-vigencia-de-ley-dicom.html>

notoriamente su efectividad jurídica y es su texto tan sucinto que para comprender el contexto dentro del cual surge la idea de legislar, es necesario recurrir a la historia de la ley[36].

[36] VIOLLIER, Pablo. El Estado de la Protección de Datos Personales en Chile. [en línea]: Derechos Digitales. 2017. [fecha de consulta: 4 octubre 2018]. Disponible en: <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf>

CAPÍTULO 4:

LA PROTECCION DE LOS DATOS PERSONALES COMO DERECHOS.

11) Ciudadanos y consumidores.

En nuestra sociedad actual, la tendencia global y nacional es que las personas se describan más como consumidores que ciudadanos pues hay mayor participación en cuanto al consumo de productos y servicios que a participar en debates políticos o votaciones electorales.[37]

Consecuencia de lo anterior es que a medida que consumimos distintos bienes y servicios, ya sea comprando con la tarjeta de crédito, dando nuestro RUT pedido por distintas tiendas para acceder a "descuentos o acumular puntos", comprando en el e-commerce, o en general para cualquier interacción que realicemos con el comercio, siempre se están acumulando datos personales en alguna base de datos. Como consumidores estamos exponiendo y entregando información personal en cuanto a nuestras preferencias y gustos, estando disponible para la empresa con la cual estamos comprando y cualquier otro tercero involucrado con aquella. Pero como ciudadanos no le tomamos real peso a esta exposición. Consecuencia de lo mencionado anteriormente es que nos encontramos muy vulnerados pues habitualmente están siendo tratados nuestros datos por agentes de comercio para fines de consumo, pero no hay ningún organismo que fiscalice o controle el uso e incluso comercio de estos datos.

En nuestro país se busca proteger las garantías de los consumidores con una institucionalidad que establece mecanismos que sean capaces de brindarles protección. Desde el año 1932 que se ha buscado proteger al consumidor, a través de la creación de distintos organismos. El más reciente es el Servicio Nacional del

[37]Felipe Harboe. Derechos del Consumidor y Protección de Datos Personales. [En línea]: Derechos Consumidor. [fecha de consulta: 4 octubre 2018]. Disponible en: <https://mba.americaeconomia.com/sites/mba.americaeconomia.com/files/derechosconsumidor.pdf>

Consumidor al cual con la promulgación de la Ley N° 19.496 sobre la Protección de los Derechos de los Consumidores, se estableció un marco normativo en cuanto a los derechos y deberes de los consumidores dándole atribuciones al SERNAC para mediar en los conflictos del consumo.

12) El Consumidor y su importancia en el flujo de datos personales.

En nuestra sociedad neoliberalista, nos encontramos constantemente comprando cosas y contratando servicios. Las personas en el diario vivir no dimensionan todos los datos personales que constantemente están exhibiendo o bien voluntariamente entregando a distintas empresas a cambio de un descuento, por ejemplo. Estos datos son almacenados en distintas bases de datos de empresas y compañías del país quienes los tratan y pueden transmitir a terceros cumpliendo con los requisitos que establece la ley, los cuales como ya comentamos en el capítulo 3, son muy poco exigentes. Es por lo que al momento de comprar estamos generando más información y mayor recopilación de datos. Somos consumidores de servicios y productos, pero a la vez somos generadores de información y de datos personales específicamente.

A medida que vamos comprando consecuencialmente se van generando nuevos flujos de datos que provienen de nosotros y van hacia las empresas, desconociendo el propósito o el uso de estos ya que a pesar de que existe el Principio de Finalidad de los Datos**,** no existe un control efectivo ni ningún organismo que pueda velar por el cumplimiento de la ley.

13) Mecanismos de Protección de los Datos Personales del Consumidor:

Recientemente la sociedad civil se ha hecho más consciente de esta situación y se han tratado de informar y defender a través de fundaciones sin fines de lucro. El Estado también ha impulsado campañas que a través del SERNAC busca proteger al consumidor, que es la persona natural que más datos personales entrega. Es menester destacar el impulso y el ánimo de modernizar la legislación actual por parte del Poder Legislativo. Esto se manifiesta a través de numerosos proyectos de ley.

13.1) Rol del SERNAC:

Dentro de las facultades del SERNAC está el de requerir información para hacer cumplir la ley, dotado por la ley N° 20.555 que le otorgó atribuciones en materias financieras a la Institución, otorgando entre otros aspectos la facultad al Servicio Nacional del Consumidor de requerir de los proveedores una serie de antecedentes adicionales a la información básica comercial. En la página web del organismo, se puso a disposición un "Manual de Requerimiento de Información" que establece cuáles son estos antecedentes que se podrán solicitar en virtud del requerimiento de información creado por la nueva legislación, el cual deberá y podrá ser utilizado por SERNAC para la ejecución y cumplimiento de sus atribuciones. Respectos de los datos personales son:

"Información relativa a la Ley N° 19.628 y sus modificaciones legales; en lo específico como da cumplimiento a velar por la seguridad de la información de los consumidores, puntualmente en el uso y destino de los datos personales, ya sea de proveedores respecto de los cuales existe un contrato, sea o no de adhesión que lo vincule con el consumidor, o bien, a proveedores de bases de datos."[38]

13.1.1) Campañas:

13.1.1.1) No Molestar:

La ley Nº 19.496 que establece normas sobre protección de los derechos de los consumidores publicada el 07 de marzo de 1997 fue modificada por la ley Nº 19.955 publicada el 14 de julio de 2004 la cual, entre muchos otros preceptos incorporó el artículo 28 B[39] que dispone el derecho al consumidor de no ser molestado o acosado

[38] SERNAC. Manual de requerimiento de información Ley 19.496. [en línea]: SERNAC. 2018. [fecha de consulta: 4 octubre 2018]. Disponible en: <https://www.sernac.cl/portal/618/articles-11833_archivo_01.pdf>

[39] "20) Agréganse, a continuación del artículo 28, los siguientes artículos 28 A y 28 B, nuevos:
Artículo 28 B.- Toda comunicación promocional o publicitaria enviada por correo electrónico deberá indicar la materia o asunto sobre el que versa, la identidad del remitente y contener una dirección válida a la que el destinatario pueda solicitar la suspensión de los envíos, que quedarán desde entonces prohibidos.
Los proveedores que dirijan comunicaciones promocionales o publicitarias a los consumidores por medio de correo postal, fax, llamados o servicios de mensajería telefónicos, deberán indicar una forma expedita en que los destinatarios podrán solicitar la suspensión de las mismas. Solicitada ésta, el envío de nuevas comunicaciones quedará prohibido.".

por distintas campañas publicitarias masivas de distintas empresas con información promocional y publicitaria.

El objetivo principal del artículo 28 B es restringir la práctica comercial de envío de SPAM porque vulnera los derechos del consumidor en cuanto a su privacidad y respecto de la libre elección del producto.

En relación con lo anterior se encuentra el concepto de “SPAM”, también conocido el correo basura que consiste en mensajes, correos e información, no solicitados ni deseados y que son enviados de manera masiva por distintas empresas. El SPAM por lo general es de naturaleza anónima, no siendo solicitado por los usuarios y se distribuye de manera masiva.

La ley contempla la posibilidad de solicitar la suspensión de los envíos al SERNAC para que efectúe esta norma. El Servicio Nacional del Consumidor para facilitar el ejercicio de este derecho creó el año 2013 una plataforma llamada: “No Molestar”, la cual permite al usuario manifestar su voluntad de suspender el envío de comunicaciones promocionales o publicitarias y así ser borrados de la lista de envíos masivos que pudiera recibir a través de llamadas, correos electrónicos, mensajería de texto, correo convencional, etc.

Para poder usar esta aplicación web el Servicio pide algunos datos personales para poder hacer viable la suspensión de publicidad no deseada, ingresando el nombre de la empresa de la cual quiere dejar de recibir estas comunicaciones publicitarias masivas. Es más, el mismo artículo 28 B garantiza que una vez suspendidas las comunicaciones por parte de una empresa, esta última no podrá volver a enviar de nuevo mensajes de esta naturaleza al mismo consumidor.

13.1.1.2) No doy mi Rut (ONG Datos Protegidos):

El artículo 4 de la ley N° 19.628 en su primer y segundo inciso señala que, *“El tratamiento de los datos personales solo puede efectuarse cuando la ley lo autorice o el titular consienta expresamente en ello. La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos*

personales y su posible comunicación al público", esto conocido como el "Principio de Finalidad".

En la práctica aquello no se respeta por el comercio que sin explicación requiere nuestros datos para realizar cualquier transacción. Actualmente se siguen cometiendo abusos y a su vez se tolera la infracción constante por parte de la sociedad civil. Por todo lo anterior es que se han impulsado campañas a través de distintas Organizaciones No Gubernamentales (ONG) y distintas entidades como, por ejemplo, Fundación Datos Protegidos, Asociación Chilena de ONG ACCION, Fundación Ciudadano Inteligente, entre otras.

Datos Protegidos es una Organización sin fines de lucro, cuya misión es la promoción, defensa y fortalecimiento de los derechos a la privacidad y protección de los datos personales como derechos fundamentales. En su página web[40] y a través de otros sitios lanzaron la campaña "#No Doy Mi Rut", señalando, "Al entregar el RUT, las empresas crean un perfil personal con tu comportamiento y privacidad, información que consecutivamente es convertida en una base de datos comercial que otras empresas compran para evaluar tu salud, educación o economía. Tu eres el producto."

Cuando vamos a comprar a alguna tienda o casa de comercio, es "natural" que nos pidan el RUT siendo una condición para poder acceder a mejores descuentos y promociones de la empresa. Esta práctica se ha hecho común en todo Chile, siendo por lo general solicitadas en cualquier categoría de tiendas, hasta de comida rápida. Lo que desconocemos es lo que pasa con esa información y como es manejada por la empresa misma.

A nuestro parecer el precio que estamos pagando al entregar casi automáticamente y de manera voluntaria nuestro RUT, es demasiado alto, debido a que en este acto estamos aceptando la recopilación y el tratamiento de nuestros datos personales por la empresa pertinente.

[40] ¿Eres un producto? [en línea]: Fundación Datos Protegidos. 2018. [fecha de consulta: 4 octubre 2018]. Disponible en: <https://datosprotegidos.org/no-doy-mi-rut/>

Pese a que el Rut es un dato accesible al público y el artículo 4 de la ley N° 19.628, en sus últimos 2 incisos señala que *"No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.*

Tampoco requerirá de esta autorización el tratamiento de datos personales que 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 aquéllos.", este es un dato personal que merece protección y mayor conciencia al momento de entregarlo, sobre todo cuando no es obligatorio, pues con ese simple dato pueden saber por ejemplo quienes son nuestros padres, hermanos, datos electorales, viajes en avión, etc. Cuidar tus datos es también cuidar tu libertad.[41].

13.2) Casos de filtración de datos personales y el rol del SERNAC como mediador:

13.2.1) Caso Claro:

En el año 2013 el SERNAC recibió una denuncia en que se señalaba que cerca de 4.200 consumidores se vieron afectados por la filtración de datos personales desde el sitio de la empresa de telecomunicaciones CLARO. Dicho lo anterior, CLARO se sometió a una mediación colectiva presidida por el SERNAC y fue en esta instancia que reconoció la filtración de los datos y se comprometió a indemnizar de los perjuicios causados a los usuarios. Todo esto se regula a través del Principio

[41] No des tu Rut. [En línea]: ONG Derechos Digitales y Noise Media. [Fecha de consulta: 4 octubre 2018]. Disponible en: <https://nodesturut.cl/>

de Finalidad que se refiere a que estos datos solo podrán usarse para los fines que el consumidor autorizó previamente[42].

13.2.3) Caso Filtración de Tarjetas de Crédito Bancarias:

A mediados de Julio del presente año se efectuó una filtración masiva a los siguientes Bancos: CMR Falabella, BBVA, BCI, Santander, Banco de Chile, Banco Falabella, Entel Visa, Banco Galicia (de Argentina), Promotora CMR, Banco Ripley, Banefe, Itaú, Scotiabank, Edwards, Chase, Banco Pichincha (de Ecuador), BICE, Wells Fargo, Security, Credichile, Neteller, CorpBanca, Coopeuch, BCI Nova, Banco Paris, Presto.

En esta filtración de la base de datos, se pudo obtener información de aproximadamente 14.000 cuentas de tarjetas de crédito, incluyendo su Nombre, Número de Tarjeta, Código de Seguridad y Fecha de expiración de esta. Según la página web de Noticias de La Tercera[43] este acto de cibercrimen se le adjudicó al grupo de hackers llamado "TheShadowBrokers", el cual fue fundado a fines del año 2015 y que también fueron los responsables de las filtraciones de la Agencia de Seguridad Nacional de Los Estados Unidos.

El 12 de septiembre del presente año a través del sitio web del SERNAC, este último informó que iniciaría mediación colectiva con Correos de Chile por filtración de datos de tarjeta de crédito. Luego que este organismo asumiera la responsabilidad en las filtraciones, con el objetivo de compensar los daños producidos a los consumidores afectados.

Es importante considerar que los consumidores afectados por las actuaciones que vulneran derechos vinculados con sus datos personales y que se encuentran regulados por la ley 19.496, pueden ejercer sus acciones de interés individual antes

[42] Servicio Nacional del Consumidor [en línea]: "Tras mediación colectiva con SERNAC: Claro compensará a consumidores afectados por filtración de datos personales". 2013 [fecha de consulta: 3 octubre de 2018] disponible en: <https://www.sernac.cl/tras-mediacion-colectiva-claro-compensara-a-consumidores-afectados-por-filtracion-de-datos-personale/>

[43] La tercera. [en línea]: "Cómo saber si te afecta la filtración de datos de tarjetas de crédito y qué hacer al respecto". 2018. [fecha de consulta: 3 de octubre de 2018] disponible en: <https://www.latercera.com/pulso/noticia/saber-te-afecta-la-filtracion-datos-tarjetas-credito-al-respecto/257916/#>

los Juzgados de Policía Local, al tenor de lo dispuesto en el artículo 50 A inciso primero, al señalar *los jueces de policía local conocerán de todas las acciones que emanan de esta ley, siendo competente aquel que corresponda a la comuna en que hubiera cometido la infracción o dado inicio a su ejecución, a elección del actor.*

Las acciones de interés individual se definen como aquellas, que se promueven exclusivamente en defensa de los derechos del consumidor afectado.

En efecto la vulneración del artículo 28b), permite al consumidor afectado, actuar en forma personal ante el Juzgado de Policía Local respectivo, con las más amplias facultades, *en su comparecencia, las partes podrán realizar todas las gestiones procesales destinadas a acreditar la infracción y a probar su derecho, incluidas las presentación, examen y tachas de testigos, cuya lista podrá presentarse en la misma audiencia de conciliación, contestación y prueba.* (artículo 50 de la ley 19.496).

El procedimiento contenido en la ley 18.287, se aplica en directa armonía con las modificaciones contenidas en la ley 19.496, sobre las acciones de interés individual de los consumidores, en lo que se refiere a los Juzgados de Policía Local.

CAPÍTULO 5:

ESCENARIO ACTUAL, CRÍTICAS A LA LEGISLACIÓN, MODELO A SEGUIR Y LOS DESAFÍOS DEL MAÑANA.

14) Críticas a la ley N.º 19.628 y comparación con el Modelo Español:

A continuación, y de manera breve sistematizaremos las principales críticas a la actual protección de datos personales en Chile que hemos ido desarrollando en este trabajo.

- La ley N°19.628 es anacrónica. Sostenemos que lo es, desde su inicio. En efecto, es una ley de año 1.999, que no cuenta con los rangos internacionales, como son los de la Unión Europea o la OCDE, pese a que, en esa época, esto ya había sido ampliamente debatido en países desarrollados que ya contaban con leyes acordes y proteccionistas.

- Solo protege a las personas naturales. La ley sobre la protección de la vida privada tiene un ámbito de protección acotado solamente a las personas naturales, dejando afuera por tanto a las personas jurídicas. Por el contrario, se ha reconocido en otras legislaciones que las personas jurídicas también cuentan con la ya mencionada autodeterminación informativa, teniendo imagen y un prestigio que debe ser protegido a través de la ley.

  Respecto a lo anterior, señala HERRERA Y NÚÑEZ, *"Brasil estima necesario, por una razón de derecho orden económico, que el derecho de acceso debe concederse inclusive a los Estados, sentando las bases de la*

reivindicación reclamada por los países del Tercer Mundo, por un derecho de inspección sobre la información acumulada, sobre todo en las grandes instituciones científicas y técnicas de los países desarrollados.

Nosotros pensamos que es indudable la necesidad de protección de datos de las personas jurídicas, sobre todo ahora que cierta información ha pasado a considerarse como un activo estratégico tan valioso como la misma materia prima o el capital. Una empresa que da información sobre sí misma tiene el mismo interés que el individuo en protegerla, sobre todo cuando se trata de secretos comerciales y no cuenta con legislación al respecto en ese país."[44]

- Permite la libre transmisión de datos personales a terceros.

  La comunicación o transmisión de datos a terceros, es la regla general en nuestra legislación, establecido en el artículo 5° de la ley para lo cual se deben cumplir 2 requisitos básicos. Los requisitos de cautelar los derechos de los titulares de datos y que la transmisión guarde relación con las tareas y finalidades de los organismos participantes, ni siquiera serán necesarios para realizar un procedimiento automatizado de transmisión en el caso de datos accesibles al público en general y respecto a las transmisiones de datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes.

  La libre comunicación de datos nos parece muy perjudicial, pues nuestro sistema legitima la transmisión, que se traduce en la comercialización y lucro de los datos personales. Es muy distinto a lo que pasa en países desarrollados (donde

[44] HERRERA BRAVO, Rodolfo y NÚÑEZ ROMERO, Alejandra. Derecho Informático. Chile: Ediciones Jurídicas La Ley, 1999. 465 p.

este tema se viene discutiendo desde hace más de 4 décadas), en los cuales la regla general es la prohibición de transmitir los datos personales.

- No contempló la protección transfronteriza de datos personales. La ley N° 19.628 es limitada. No cuenta con los estándares de las normativas europeas y específicamente no contempla normas relativas al flujo transfronterizo de datos. La ley chilena queda reducida en cuanto a su efectividad de proteger nuestros datos personales, pues no hay norma que impida transferir los datos a países que no cuenten con la protección de estos ni un sistema sancionatorio por el uso de los datos personales fuera de nuestras fronteras.

- Es ineficaz. a ley no cumple con el objetivo de proteger la vida privada, ya que se preocupa solamente del tratamiento de los datos personales dejando fuera la vida privada y la intimidad.

- No existe Agencia de Datos Personales**.** La Leges Data, respecto del registro del tratamiento de los datos personales no estableció ningún organismo o agencia de control que ejerciera las facultades fiscalizadoras. Como comentamos en su oportunidad, existe un proyecto de ley (Boletín N° 11092-07) y su idea original era crear la agencia de protección de datos, lo cual fue modificado por indicaciones del presidente Sebastián Piñera. Actualmente piensa entregarse aquella facultad al Consejo para la transparencia.

- No existe un registro general de bases de datos. No existe un registro general de bases de datos en Chile. Por ley solo las bases de datos a cargo de órganos públicos deben ser inscritas en un registro a cargo del Servicio de Registro Civil e Identificación. En cambio, las bases de datos de los organismos privados no se encuentran registradas ni reguladas propiamente tal.

  La excepción de datos adquiridos de fuentes accesibles al público es muy amplia. La frase de que no se aplicará la regla pertinente en caso de que sean datos accesibles al público, se encuentra presente en varios artículos a lo largo de la ley. Creemos que es su falencia más importante, pues aquella excepción desvirtúa todo espíritu de protección.

Enumeraremos los casos que vemos a lo largo de la ley N° 19.628 que ejemplifican que la regla general de resguardo se ve sobrepasada por la amplísima excepción de los datos adquiridos de fuentes públicas. Aquello se traduce en nuestra opinión, en la venia del tratamiento de datos sin restricciones porque además su definición es poco precisa. A saber:

i. En su artículo 4° señala como regla general que los datos se pueden tratar cuando lo autorice la ley o el titular consienta expresamente, pero en su inciso 5° señala que no requiere autorización el tratamiento de datos que se recolecten de fuentes accesibles al público.
ii. El artículo 5° establece los 2 requisitos para establecer la transmisión de datos señalando además que el receptor solo puede utilizar los datos para los fines que motivaron la transmisión, pero en su penúltimo inciso señala que no se aplicará el artículo cuando se trate de datos personales accesibles al público en general.
iii. El artículo 7° establece el deber de secreto para las personas que trabajan en el tratamiento de datos personales que hayan sido recolectados de

fuentes no accesibles al público, dejando fuera a los de fuente de acceso público.

iv. El artículo 9° establece que los datos personales deben utilizarse solo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público. Nuevamente señala que, si los datos son públicos, se exceptúa a esta protección y finalidad de datos.

Sumado a lo anterior, la definición de fuentes accesibles al público del artículo 2° letra i) de la ley N° 19.628 es pésima porque da una definición muy vaga: *"Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes",* dando cabida a que diversas cosas puedan ser datos públicos, es más, las personas y empresas dedicadas al comercio de datos personales se suelen excusar de que tratan datos públicos. Es muy distinto a lo que ocurre en España, que tiene establecido un catálogo taxativo de todas las fuentes públicas.

Las sanciones son extremadamente bajas, en efecto en el artículo 16° de la ley 19.628 establece como multas de 1 a 10 UTM y de 10 a 50 UTM respectivamente, las cuales como ya habíamos comentado son extremadamente bajas y no representan ningún incentivo para cumplir con la ley, pues los beneficios que pueden con este negocio ilícito son inconmensurables.

Distinto a lo que pasa en España en que las multan son extremadamente altas. En Chile la mayor multa asciende a aproximadamente 2.417.650 pesos chilenos, en cambio el monto máximo dispuesto en la ley española asciende a 300.000.000 de pesos chilenos.

- No se estableció responsabilidad objetiva. La ley N° 19.628 estableció un sistema de responsabilidad civil basado en la culpa del responsable de la base de datos, en vez de un sistema de responsabilidad

objetiva, lo que se traduce en la carga de la prueba en la víctima, siendo prácticamente imposible acreditar la culpa o negligencia.

15) Consentimiento en la era cibernética:

Pese a que el consentimiento en internet está lejos de ser regulado en nuestro país, queremos realizar un breve comentario debido al gran alcance e importante que tienen.

La exposición de las personas en las Redes Sociales es normal en “la sociedad de la información”, pero tenemos poca conciencia de la implicancia que tienen nuestros datos personales que cotidianamente exponemos con el uso del celular y las distintas aplicaciones disponibles. A modo de ejemplo, una simple búsqueda de Google o de un amigo en Facebook, genera información que está siendo constantemente almacenada y tratada por las empresas mencionadas anteriormente. Esto no solamente se limita a los datos personales clásicos, sino también al contenido multimedia como fotos y videos que, si son identificados con una persona determinada o determinable, también son datos personales.

A modo de comentario, el año 2013 se estrenó un documental en Netflix, que se titula “Pueden aplicar términos y condiciones” que, entre varios otros temas, señala que las empresas como Facebook y aplicaciones de similar naturaleza, tienen como negocio principal la recopilación de toda la información posible de los usuarios que interactúen con sus plataformas. A continuación, con esta información recopilada se realizan distintos perfiles en base a las preferencias y gustos de los usuarios, bajo la excusa de “agilizar el funcionamiento de las aplicaciones y proteger a los usuarios”. Los términos y condiciones son contratos de adhesión que uno acepta con un clic, los cuales casi nadie lee. Asimismo, el documental señala que las políticas de privacidad han ido cambiando y actualmente la regla general es que todo contenido sea público, debiendo la persona configurar la aplicación para hacer el contenido privado.

La principal consecuencia de lo anterior es la “Irreversibilidad de nuestra huella digital”, pues cada vez que publicamos o subimos contenido a estas aplicaciones, no importa si luego las eliminamos, ésta quedará para siempre registrada en el mundo virtual. Son las mismas empresas como Google, Facebook, Twitter, Instagram entre otros que registran todas las publicaciones y contenido que se suban a estas plataformas, siendo almacenadas en sus bancos de datos.

Como usuarios al aceptar los mencionados términos y condiciones estamos transfiriendo, cediendo y entregando toda nuestra información personal y no solamente eso, sino que también autorizando a la empresa a que sea recopilada, tratada e incluso siendo transferida a terceros interesados para distintos fines. No habría problema con el uso de estos datos, porque nosotros los usuarios aceptamos entregarlos voluntariamente y de manera gratuita, todo esto al momento de hacer clic en “Aceptar los términos y condiciones.” Producto de lo anterior podemos decir que estamos transando nuestra privacidad e intimidad por poder usar una aplicación de manera gratuita o acceder a mejores descuentos u ofertas.

16) Desafíos del Mañana: “Producto Humano”

A lo largo de la presente tesis hemos tratado respecto a los datos personales y como estos son obtenidos, tratados y utilizados. Es común que empresas o corporaciones cuenten con bases de datos y que hagan uso de estas a su discreción. Consecuencia de esto es que estas empresas pueden usar indebidamente nuestros datos e información para obtener mayor captación de clientes o tratar de buscar una fidelización por parte de mejores ofertas y descuentos.

Como señala HERRERA y NÚÑEZ*, “La informática es un nuevo tipo de riqueza, ya que gracias a ella la información se ha convertido en una especie de materia prima susceptible de aprovecharse”*[45], por lo tanto, no podemos dimensionar realmente cuanta de nuestra información está expuesta para cualquier tercero o agente de comercio que la requiera. Tenemos una ley que protege a los datos personales pero que al no contar con un órgano que la fiscalice y que vele su aplicación, además de

[45] HERRERA BRAVO, Rodolfo y NÚÑEZ ROMERO, Alejandra. Derecho Informático. Chile: Ediciones Jurídicas La Ley, 1999. 465 p.

no existir un control sobre el flujo de datos transfronterizo, en consecuencia, quedamos desprotegidos no solo en nuestro país, sino que para el mundo entero.

Pero ¿a qué le llamamos Producto Humano? Somos productos de nuestras preferencias, de lo que compramos o necesitamos. Al final del día cada transacción, cada compra que realizamos en distintas empresas, quedan registradas en sus bases de datos. A través del RUT distintas empresas realizan verdaderos perfiles de personas, asociando cuales son las cosas que usualmente compran. Asimismo, utilizan distintas herramientas para "fidelizar" al cliente, a través de canje de puntos, envío de correos electrónicos con especiales ofertas, entre otras. Esto es una constante que va en aumento no solo en Chile, sino que a nivel mundial. Cada vez es más común encontrarse con estas situaciones en el resto del mundo, filtración de datos personales o hackeos masivos a distintas cuentas o aplicaciones, comienzan a ser lo normal en nuestro diario vivir y la constante interrogante a esto es, quien es el encargado de regularlo, si los usuarios no tienen conocimiento ni control de donde tienen sus datos guardados o cuales empresas son las que almacenan esta información. Sabemos que estas últimas tienen estos datos y que constantemente almacenan, pero la forma en que son tratados estos datos es dudosa.

Es por lo último que se producen situaciones de comercialización de datos personales entre otras situaciones transgresoras de las garantías constitucionales. Todo aquello por la ausencia de una legislación moderna que no ha incorporado de manera efectiva los principios de los convenios suscritos sumado a la historia de la ley, donde deja vislumbrar que se aprobó una ley de datos personales que legalizó el derecho que tienen las personas a realizar tratamiento de datos personales, con la ausencia de un marco normativo protector de sus titulares. Durante la tramitación y promulgación de la ley, se hizo lobby por parte de las empresas para facilitar la recopilación de datos por parte de ellos y no realmente proteger la vida privada y los datos personales de las personas naturales como era el espíritu de esta.

CONCLUSIONES.

A lo largo del presente estudio, pudimos concluir que son escasas las investigaciones que existen sobre los datos personales en Chile y lo que es más grave aún, sobre el derecho a la privacidad e intimidad. No todas las personas titulares de datos personales conocen sus derechos y los responsables de datos personales no conocen bien sus obligaciones. Creemos que este desconocimiento civil se debe en parte a la falta de investigación y desarrollo doctrinario de este tema en Chile, sumado a la falta de campañas para promover los derechos a la protección de la vida privada, en especial sobre los datos personales.

En nuestro país la protección de los datos personales parece un desafío no logrado, pues se ha tratado de priorizar su discusión y tramitación en el congreso, pero sin resultados efectivos ya que el tratamiento, la regulación y la protección de los datos personales no cuentan con un marco normativo necesario para proteger de manera correcta y eficaz este bien jurídico.

Somos un país en vías de desarrollo que cuenta con alta tecnología, pero no con una legislación acorde a los estándares internacionales que garantice la privacidad y la protección de los datos personales. La situación se agrava por los avances tecnológicos que nos expone a nuevos riesgos, sobre todo, internet que facilita la recolección y tratamiento de aquellos, dando origen a situaciones muchas veces irregulares como lo son su comercialización, permitido por nuestra legislación, incluso sin el consentimiento del titular cuando estos datos sean de libre acceso público.

Respecto a su reciente consagración constitucional, a 6 meses de aquello no existe certeza sobre su incidencia. Creemos que aquello dependerá de los proyectos de leyes que se aprueben a corto plazo, pues su consagración señala que *"El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley",* pero como ya analizamos, la ley N° 19.628 es defectuosa, incompleta y anacrónica.

Creemos que es fundamental la creación, desde cero, de una nueva ley que contenga un espíritu de verdadera protección a sus titulares. Todo lo contrario, a la actual ley que fue tramitada bajo un contexto de gran lobby por parte del empresariado para legitimar la comercialización de los datos personales. Prueba de aquello es que el 1° artículo de la ley citada en su 2° inciso consagra el derecho que tiene toda persona para efectuar el tratamiento de estos, antes que establecer la protección a sus titulares.

Proponemos a corto plazo una ley que modifique los bajísimos montos de las sanciones pecuniarias estableciendo multas que signifiquen un incentivo para cumplir la ley. Un gran estímulo, a nuestro parecer sería una multa de 500 UTM. También, proponemos que se restrinjan las excepciones de datos obtenidos de fuentes de acceso público, es decir, que se deroguen de la ley 19.628 los incisos 5° del artículo 4°, el penúltimo inciso del artículo 5°, la segunda parte del artículo 7° que deja fuera el deber de secreto cuando sean datos recolectados de fuentes de acceso público y el artículo 9° que de la misma forma exceptúa del principio de finalidad la protección de aquellos datos. Creemos que es muy importante además que se modifique la definición de fuentes accesibles al público del artículo 2° letra i) que es genérica y ambigua, por una más concreta con una enumeración taxativa de sus excepciones para así limitar su comercialización. Más urgente, es la creación de una ley que limite la transmisión de datos a terceros, que permite nuestra legislación en su artículo 5° para así disponer la prohibición de la transmisión como regla general, tal como lo han reglado la mayoría de los países desarrollados.

Nuestra visión es proteccionista pues nos resulta fundamental nuestro derecho a la privacidad y vida privada sobre el derecho a ejercer la libertad de opinión e información y de desarrollar cualquier actividad económica. En consecuencia, planteamos a largo plazo una nueva legislación y no leyes “parches”. Proponemos un nuevo marco legal que efectivamente incorpore los principios de datos personales reconocidos por Chile, restrinja las excepciones de datos públicos, establezca taxativamente fuentes accesibles al público, limite su comercialización,

trate el flujo transfronterizo de datos personales, aumente el valor de las multas y cree una autoridad de control que fiscalice el cumplimiento de la ley.

BIBLIOGRAFÍA.

ALVARADO ÁLVAREZ, Francisco. Internet y las fuentes de acceso público a datos personales. (Licenciado en Ciencias Jurídicas). Santiago, Chile: Universidad de Chile, escuela de Derecho. 2013. 194 pág.

ANGUITA RAMÍREZ, Pedro. La protección de datos personales y el derecho a la vida privada. Editorial Jurídica de Chile, Santiago, Chile, 2007, pág. 627.

ARRIETA, Raúl. Chile y la protección de datos personales: compromisos internacionales, pp-13-22. En: VVAA. Chile y la protección de datos personales: ¿están en peligro nuestros datos personales? Santiago, Ediciones Universidad Diego Portales. 2009, 102 pág.

Biblioteca del Congreso Nacional de Chile [en línea] "Guía Legal sobre Ley Dicom". 2012. [fecha de consulta: 2 de octubre del 2018]. Disponible en <http://www.bcn.cl/leyfacil/recurso/ley-dicom>

DE LA SERNA BILBAO, María Nieves. La institucionalización de la protección de datos de carácter personal. En: Reflexiones sobre el Uso y Abuso de los Datos Personales en Chile. Santiago: Expansiva, 2011. Pp. 55-77.

Emol [en línea]: "Denuncian nueva infracción de Equifax a días de la entrada en vigencia de "Ley Dicom". 2012 [fecha de consulta: 3 octubre de 2018] disponible en:
<https://www.emol.com/noticias/economia/2012/03/02/528908/denuncian-nueva-infraccion-de-equifax-a-dias-de-la-entrada-en-vigencia-de-ley-dicom.html>

HERRERA BRAVO, Rodolfo y NÚÑEZ ROMERO, Alejandra. Derecho Informático. Chile: Ediciones Jurídicas La Ley, 1999. 465 p.

La tercera. [en línea]: "Cómo saber si te afecta la filtración de datos de tarjetas de crédito y qué hacer al respecto". 2018. [fecha de consulta: 3 de octubre

de 2018] disponible en: <https://www.latercera.com/pulso/noticia/saber-te-afecta-la-filtracion-datos-tarjetas-credito-al-respecto/257916/#>

Servicio Nacional del Consumidor [en línea]: “Tras mediación colectiva con SERNAC: Claro compensará a consumidores afectados por filtración de datos personales”. 2013 [fecha de consulta: 3 octubre de 2018] disponible en: <https://www.sernac.cl/tras-mediacion-colectiva-claro-compensara-a-consumidores-afectados-por-filtracion-de-datos-personale/>

UÑE LLINAS, Emilio. Tratado de Derecho Informático: Introducción y protección de datos personales. “Sobre las primeras iniciativas parlamentarias en la materia”. MADRID. Universidad Complutense, Servicio de Publicaciones. Año 2000. Volumen 1.

VIOLLIER, Pablo. El Estado de la Protección de Datos Personales en Chile. [en línea]: Derechos Digitales. 2017. [fecha de consulta: 4 octubre 2018]. Disponible en: <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf>

LEYES Y REGLAMENTOS DE CHILE:

- Ley N° 19.628

- Ley N° 19.812

- Ley N° 20.575

- Ley N° 20.521

- Ley N° 21.096

- Ley N° 19.496

- Ley N° 18.287

- Constitución Política de la República

UNIÓN EUROPEA

- Directiva Europea 95/45/CE

- Reglamento 2016/679

ESPAÑA

- Ley N°5/1992

- Ley N°15/1999