UNIVERSIDAD DE CHILE

FACULTAD DE DERECHO

DEPARTAMENTO DE DERECHO PRIVADO

RÉGIMEN DE INDEMNIZACIÓN DE PERJUICIOS DE LA LEY N°19.628 Y LA SEGURIDAD DE DATOS PERSONALES

Análisis crítico del principio de seguridad de datos del artículo 11° de la Ley de Protección a la Vida Privada y su aplicación práctica.

Tesis para optar al grado de Licenciado en Ciencias Jurídicas y Sociales

AUTOR:
Sebastián Alonso Peña Yáñez

PROFESORA GUÍA:
María Magdalena Bustos Díaz

Santiago, Chile

2019

A mi mamá y a mi papá, ya que sin todo lo que me han dado no estaría escribiendo estas líneas hoy.

A Lucas, Noah y Elvis, por su compañía.

A Sofía, por todo su cariño.

TABLA DE CONTENIDOS

RESUMEN

En el presente trabajo se analiza el principio de seguridad de datos personales de la Ley N°19.628 Sobre Protección de la Vida Privada y la responsabilidad civil del responsable de datos derivada de la inobservancia del deber de adopción de medidas de seguridad. Para ello se revisa el marco normativo general de la protección de datos personales en Chile, para posteriormente centrarse en el estudio del régimen de responsabilidad civil que la mencionada ley regula en su artículo 23°, presentando sus generalidades y falencias. Luego de esto, se trata en específico el principio de seguridad de datos personales, identificando su adopción en el artículo 11° de esta ley y ofreciendo una interpretación de éste que implica concluir que el debido cuidado de los datos personales supone la adopción de medidas de seguridad que, de no cumplirse, puede acarrear la responsabilidad civil del responsable de datos. A la vez, para su desarrollo, el presente trabajo se apoya en la doctrina nacional y comparada al respecto, así como en el derecho comparado pertinente.

INTRODUCCIÓN

Hoy en día nos encontramos inmersos en una sociedad que se encuentra digitalizada casi en su totalidad. Desde los grandes procesos industriales, las elecciones presidenciales de una potencia mundial o, inclusive, algo tan común como comprar en una tienda de centro comercial, todo se encuentra permeado por las tecnologías de la comunicación e información. En este mundo digitalizado, la información es clave para una gran variedad de labores, pero al pensar en información no se debe reducir únicamente a cuestiones estadísticas, datos científicos o similares, ya que la persona humana conlleva de por sí un conjunto de información. La información relativa a esta última clase, es lo que desde ya el siglo pasado se ha conocido como "dato personal", terminología que alude a la información que hace referencia a las personas naturales.

Como nos encontramos en un mundo en que el intercambio de información permea todos los aspectos de la vida, la privacidad del ser humano tiene un rol central, ya que en nuestra sociedad actual el derecho fundamental a la vida privada no se agota en la prohibición de injerencia de la esfera de privacidad de una persona, sino que puede entenderse que hay un aspecto de ella que se juega fuera de este ámbito debido a la información que alude a nuestra persona y que está en manos de otros por su constante ir y venir. De esta forma, ante esta problemática comenzaron a proliferar por el mundo normativas de rango legal y constitucional, las cuales buscan garantizar la protección de la información personal y regularizar el tratamiento que de ella se realice.

En la actualidad la ley que trata este tema en nuestro país es la Ley N° 19.628 o "Ley de Protección de la Vida Privada", que comúnmente es conocida como la "Ley de Protección de Datos Personales". Esta normativa data del año 1999, encontrándose en profunda anacronía respecto al fenómeno del tratamiento de datos que se da el día de hoy, no respondiendo con la realidad de las tecnologías de la información y comunicación[1], la

[1] Podemos entender tecnologías de la información y la comunicación como "*todos aquellos medios de comunicación y de tratamiento de la información que van surgiendo de la unión de los avances propiciados por el desarrollo de la tecnología electrónica y las herramientas conceptuales, tanto conocidas como aquellas otras que vayan siendo desarrolladas como consecuencia de la utilización de estas mismas nuevas tecnologías y del avance del conocimiento humano*" MARTÍNEZ, F. 1996. La enseñanza ante los nuevos canales de información. En: TEJEDOR, F. J. y GARCÍA, A.: Perspectivas de las nuevas tecnologías en la educación. Madrid. Narcea, 109p. Citado en: BAELO, R. y Cantón, I. 2009. Las tecnologías de la información y la comunicación en la educación superior. Estudio descriptivo y de revisión. 2p. [en línea] <https://rieoei.org/historico/deloslectores/3034Baelo.pdf> [Consulta: 17 de marzo de 2020].

utilización de *big data*[2], el internet de las cosas[3], la proliferación del fenómeno hacker[4], entre muchas otras cuestiones que no tenían la misma naturaleza hace veinte años.

Particularmente, esta anacronía la podemos relacionar con el gran valor que hoy en día tiene la información personal y que no tenía hace un par de décadas, ya que, precisamente, por el desarrollo tecnológico, la industria del tratamiento de datos ha ido desarrollándose, siendo cada vez mayor su preponderancia dentro de la economía mundial. Hoy en día nos movemos en una economía en que los datos son un activo de mercado que se transa para fines económicos y comerciales, moviendo mercados e influyendo de forma clara en su desempeño.

Derivado de este alto valor de los datos personales es que surge la interrogante respecto de su seguridad, ya que precisamente por esta característica es que son un blanco predilecto de hackers y/o cualquier individuo en general que podría sacar provecho de ellos. De igual forma, la información personal que otros manejan respecto de las personas no únicamente se puede reducir a materias económicas, como lo podrían ser los datos relativos a tarjetas de crédito o cuentas bancarias, sino que también respecto de aspectos especialmente sensibles de las personas, como pueden ser sus datos de salud, su origen étnico o preferencias políticas. No hay lugar a dudas que la información debiese de ser resguardada para proteger a las personas de las filtraciones o utilizaciones maliciosas de su información personal, ya que este tipo de acciones pueden conllevar serios daños para una persona.

Es en este contexto que este trabajo busca analizar el artículo 11° de nuestra ley de protección de datos personales, el cual indica que el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.

---

[2] Podemos entender big data como "*activos de información caracterizados por su volumen elevado, velocidad elevada y alta variedad, que demandan soluciones innovadoras y eficientes de procesado para la mejora del conocimiento y la toma de decisiones en las organizaciones*". Véase: MATÉ, C. 2014. Big data un nuevo paradigma de análisis de datos. 10p. [en línea] <https://www.iit.comillas.edu/docs/IIT-14-153A.pdf> [consulta: 17 de marzo 2020]

[3] Internet de las cosas puede entenderse como "*una tecnología basada en la conexión de objetos cotidianos a Internet que intercambian, agregan y procesan información sobre su entorno físico para proporcionar servicios de valor añadido a los usuarios finales*". Véase: BARRIO, M. 2018. Internet de las cosas. Madrid. Editorial Reus. 19p.

[4] Podemos entender hacking como "*un conjunto de técnicas para acceder a un sistema informático sin autorización*". Véase: GIMÉNEZ, V. 2011. Hacking y ciberdelito. 13p. [en línea] <https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf> [consulta: 17 de marzo de 2020]

Particularmente, salta a la vista la determinación de si este deber de cuidado supone la adopción de medidas de seguridad de datos personales por parte del responsable, ya que, a diferencia de cómo se realiza en legislación comparada, en nuestro país no existe norma alguna que en forma expresa indique qué se entiende, si deben adoptarse, ni cómo deben de ser las medidas de seguridad de datos que, precisamente, apuntan a garantizar el cuidado de la información personal que se encuentra en manos del responsable de datos personales.

La indeterminación de un deber de adopción de medidas de seguridad por parte de una legislación puede suponer un serio riesgo de las personas, ya que es evidentemente peligroso el que las bases de datos sean fáciles de vulnerar, siendo mayor la posibilidad de que ocurran perjuicios derivados de esta situación.

Nuestra hipótesis es que, si bien nuestra legislación no especifica ni trata las medidas de seguridad de datos personales, sino que solo hace referencia a la debida diligencia en su cuidado, derivado de la interpretación del artículo 11° de la Ley Sobre Protección de la Vida Privada, podemos concluir que sí existe un deber de adopción de medidas de seguridad por parte del responsable.

Lo que resultaría problemático en esta situación es lo breve de la disposición y el no tratamiento expreso de la seguridad de datos en nuestra legislación, que, si bien puede generar problemáticas para los derechos de las personas, no significa que no se deban adoptar medidas de seguridad para el cuidado de los datos, cuestión que podemos desprender de la interpretación del artículo anteriormente mencionado.

Para lograr esto, analizaremos la doctrina y legislación nacional, así como las fuentes comparadas, a fin de poder realizar un estudio de la normativa de la protección de datos en forma general, para luego analizar el régimen de indemnización de perjuicios y el deber de seguridad de datos personales.

En este sentido, el presente trabajo se estructura en cuatro capítulos. En el primero de ellos lo que se busca es ofrecer una revisión general del marco jurídico de la protección de datos, analizando antecedentes históricos de esta rama de estudio, y revisando cuál es marco regulatorio actual de nuestro país.

Por su parte, en el segundo capítulo aterrizaremos nuestro análisis en el régimen de indemnización de perjuicios de la Ley N°19.628, para revisar cómo se acciona por

infracciones a las disposiciones de esta norma, buscando delimitar el régimen de responsabilidad civil al que se adscribe.

Una vez revisados estos temas, en el tercer capítulo abordaremos específicamente la seguridad de datos personales y buscaremos analizar su contenido, existencia en nuestra normativa y su tratamiento comparado. Directamente relacionado a lo anterior, en el capítulo cuarto realizaremos una evaluación crítica de la seguridad de datos en nuestro país y nos centraremos en el deber de conducta que supone la adopción de medidas de seguridad de datos, según el artículo 11° de la Ley N°19.628.

El tema de estudio de este trabajo encuentra su justificación, precisamente, en la importancia que hoy en día tiene la información personal y la necesidad de su protección. Nos parece particularmente problemático el hecho de que un responsable de datos no deba, al menos por imperativo legal adoptar medidas de seguridad y que no responda por los daños en caso de no haber cuidado los datos con la debida diligencia.

En ese sentido, el hecho fáctico que impulsó este interés particular fue lo ocurrido con las brechas de seguridad informáticas en instituciones bancarias durante 2018, en que se sucedieron una serie de problemas de ciberseguridad en varios bancos nacionales y que, en el caso más importante, supuso la pérdida de cerca de diez millones de dólares por parte del Banco de Chile.

Esta situación acaparó las voces de diferentes actores (académicos, autoridades, organismos de protección a los consumidores) exigiendo la responsabilidad de los bancos a la hora de que se viese filtrada la información personal de sus clientes, pero toda la discusión giraba en torno a otros cuerpos normativos (como puede ser la Ley N°19.496, que Establece las Normas Sobre Protección a los Consumidores) y en momento alguno se mencionó el artículo 11° de la Ley de Protección de Datos, que impone una exigencia de debido cuidado de los datos. De esta manera, creemos que es necesario un trabajo de análisis que pretenda ofrecer una interpretación de la normativa de protección de datos que importe la exigencia de un deber de seguridad de datos por parte del responsable.

A su vez, con este trabajo buscamos ofrecer una revisión general de la Ley N°19.628, que luego recaiga particularmente en su régimen de indemnización de perjuicios. Fue un hecho notorio la existencia de un tratamiento doctrinario más bien limitado de este aspecto específico de nuestra legislación de protección de datos en comparación a otros, por lo que nos es particularmente interesante realizar este estudio para analizar las implicancias

prácticas y problemáticas del ejercicio de la indemnización de perjuicios derivada de infracciones a nuestra ley de protección de datos.

Finalmente, también queremos destacar que hoy en día ya se discute en el Congreso Nacional un proyecto de ley que busca modificar íntegramente la protección de datos en nuestro país (proyecto al que también aludiremos en las páginas finales de este trabajo), por lo cual un estudio en una materia problemática de nuestra legislación es de total actualidad y que nos permite visualizar cuáles podrían ser las modificaciones legislativas necesarias al respecto.

CAPÍTULO I: LA LEY N°19.628 SOBRE PROTECCIÓN DE LA VIDA PRIVADA

1. LA LEY N°19.628

Para comenzar este trabajo, en este capítulo presentaremos los principales puntos a tener en consideración para entender la regulación de la protección de datos personales en nuestro país, por lo cual es necesaria una revisión general de la Ley N°19.628 Sobre Protección de la Vida Privada, delimitando sus ideas matrices, conceptos, principios y ámbitos de aplicación.

La Ley N°19.628 Sobre Protección de la Vida Privada (en adelante "LPD") tuvo su origen en moción parlamentaria[5] presentada en el Senado en enero de 1993, teniendo como propósitos originales: el solventar un vacío en el ordenamiento jurídico nacional mediante el establecimiento de una adecuada protección al derecho a la vida privada de las personas en sus diversos aspectos en el ámbito del derecho civil; introducir algunos mecanismos e instrumentos específicos de protección frente a las intromisiones ilegítimas y los instrumentos de compensación ante los daños que eventualmente puedan producirse; y la intención de consagrar una suerte de "código" o estatuto jurídico de la privacidad en nuestro país, de modo que un texto refundido, coordinado y sistematizado terminase con la dispersión de normas legales en las distintas ramas de nuestro ordenamiento.

El proyecto contemplaba disposiciones que especificaban la extensión del concepto jurídico de vida privada (incluyendo los derechos a la propia imagen, intimidad personal y familiar, anonimato o reserva, vida tranquila sin hostigamientos ni perturbaciones; así como inviolabilidad del hogar y de toda otra forma de comunicaciones privadas), prohibía intromisiones ilegítimas a esta esfera, establecía mecanismos de protección frente a éstas, y otorgaba instrumentos de compensación ante eventuales daños morales y materiales producto injerencias ilegítimas. Dentro de sus puntos, se contemplaba un Título II denominado "De la Protección de Datos", que luego de que la moción fuese discutida por la Cámara de Diputados, quedó como el único ámbito al que se circunscribió la ley. De allí es que resulte extraño el nombre "Sobre Protección de la Vida Privada", cuando únicamente se refiere a un solo aspecto derivado de ésta, que es la autodeterminación informativa en lo que respecta al tratamiento de datos personales.

[5] Boletín N°896-07 "Proyecto de ley sobre protección civil de la vida privada".

Es muy importante precisar las diferencias existentes entre los conceptos de vida privada y protección de datos personales, ya que permite entender la lógica que existe detrás de la proliferación de las regulaciones de datos personales. En este punto, desde hace siglos, la configuración jurídica de un derecho a la privacidad ha sido entendida en base a la reserva de aspectos de la vida personal que legítimamente se excluyen de la injerencia de terceros, evolucionando desde el clásico "*right to left alone*" de Brandeis y Warren[6], a ser reconocido internacionalmente en instrumentos tan importantes como la Declaración Universal de Derechos Humanos[7], así como estar presente, explícita o implícitamente, en las distintas Constituciones Políticas de los Estados. No obstante, la proliferación de los medios de comunicación de masas y el vertiginoso desarrollo de las tecnologías de la información han puesto en jaque las posibilidades de la protección de la privacidad de las personas, ya que se ha generado una inimaginable capacidad para recoger, procesar y transmitir información, lo que ha provocado la necesidad de poder limitar y controlar la información concerniente a la persona que es objeto de distintos tratamientos. En estas condiciones, la intromisión de la informática y las telecomunicaciones en el diario vivir de las personas motivó a una ampliación o reformulación conceptual del derecho a la intimidad, planteándose como "*el derecho del individuo a decidir por sí mismo en qué medida quiere compartir con otros sus pensamientos y sentimientos, así como los hechos de su vida personal*"[8].

Entendida de esta forma, la protección de la vida privada pasó de una faz negativa del derecho, en el sentido de imponer límites a las injerencias que terceros podrían realizar a una esfera de privacidad, a una faceta positiva del derecho, confiriendo una serie de facultades para controlar la información personal que puede ser tratada y accedida por los demás. De ello, ante la necesidad de proteger los intereses de los individuos en miras a controlar la información que terceros poseen de ellos, es que surge el concepto de autodeterminación informativa, libertad informática o privacidad informacional.

[6] WARREN, S. y BRANDEIS, L. 1890. The Right to Privacy. En: Harvard Law Review 4(5): 93-220.
[7] *Artículo 12°: Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*
[8] CERDA, A. 2012. Legislación sobre protección de las personas frente al tratamiento de datos personales. Santiago, Centro de Estudios de Derecho Informático de la Facultad de Derecho de la Universidad de Chile p.7.

En específico, en doctrina[9] se ha entendido que fue el Tribunal Constitucional Alemán, al anular la Ley de Censo de Población de 1982, quien por vez primera le dio reconocimiento jurisprudencial al "derecho a la autodeterminación informática" como categoría jurídica autónoma, con tal de explicar la tutela otorgada a las personas ante el tratamiento automatizado de sus datos. Esta sentencia[10] configura el derecho a la autodeterminación informativa, indicando que el individuo tiene la facultad, derivada de su autodeterminación, de decidir por él en qué momento y dentro de qué límites es procedente revelar antecedes referentes a su propia vida, fallando que la mencionada ley de censo importaba una afectación contra la posibilidad de que el ciudadano censado pudiera controlar la información que estaba suministrando. Más adelante, la jurisprudencia al respecto proliferaría en distintos países, principalmente en Europa, entre las que podemos destacar las sentencias emitidas por el Tribunal Constitucional de España[11].

Por otra parte, existe bastante desarrollo doctrinario de este derecho, pudiendo citar a autores como Emilio Suñé, quien identifica la estrecha relación existente entre intimidad y autodeterminación informativa, al indicar que ésta es una forma de referirse a las particulares características que adquiere el derecho a la intimidad en la era informática[12]. De igual forma, Ana Herrán nos señala que el derecho a la autodeterminación informativa se identifica con la libre capacidad de decisión que todo individuo ostenta respecto de la difusión, utilización y cesión de la información que le concierne[13]. A su vez, también podemos mencionar a Murillo de la Cueva, que esboza que el derecho a la

[9] En este sentido, véase: MURILLO DE LA CUEVA, P. 2008. El derecho a la autodeterminación informativa y la protección de datos personales. En: Azpilcueta: Cuadernos de Derecho(20): 44p.
En igual sentido, véase: CERDA, A. 2003. Intimidad de los trabajadores y Tratamiento de datos personales por los empleadores. En: Revista Chilena de Derecho Informático(2): 35-59.

[10] Tribunal Constitucional Alemán, sentencia de 15 de diciembre 1983.

[11] Ejemplo es su sentencia 11/1984, de 26 de noviembre, dictada con motivo de un recurso de amparo debido a la vulneración del derecho a la privacidad por la exigencia de aportar certificaciones de las operaciones de determinadas cuentas bancarias. Principalmente, la sentencia arguye que es necesario ampliar las fronteras respecto a la protección de los derechos del individuo, debido a que el concepto de vida privada o de "calidad de vida" no había permanecido inalterable con los años, sino que se puede afirmar que el ser humano adquiere nuevas pretensiones respecto a su esfera de intimidad con el paso del tiempo. Véase: ZABALLOS, P. 2013. La protección de datos personales en España: evolución normativa y criterios de aplicación. Memoria para optar al grado de Doctor en Derecho. Madrid, Universidad Complutense de Madrid, Facultad de Derecho. 72-75pp.

[12] SUÑÉ, E. 2000. Tratado de Derecho Informático. Introducción y protección de datos personales. Madrid. Servicio de Publicaciones Universidad Complutense de Madrid. Vol.1. 29p. Citado en: JERVIS, P. 2006. La regulación del mercado de datos personales en Chile. Tesis para optar al grado de Magíster en Derecho. Santiago, Universidad de Chile, Facultad de Derecho. 44p.
Esta tesis de Jervis es, a nuestro parecer, uno de los mejores trabajos que existen en el país respecto a la regulación de los datos personales, por lo que volveremos a él en varias oportunidades, principalmente por su excelente documentación al respecto.

[13]HERRÁN, A. 2002. El Derecho a la Intimidad en la nueva ley orgánica de protección de datos personales. Madrid, Dykinson. 68p. Citado en: JERVIS, P., *loc. cit.*

autodeterminación informativa se construyó sobre la base del derecho a la intimidad, tanto como este último lo hizo sobre la base del derecho de propiedad en su momento[14]. A mayor abundamiento, en Chile, Rostión propone que surge del derecho a la intimidad, pero con un sello identitario propio, ya que derivaría de las posibilidades que existen en la actualidad de que la agresión informática vulnere una multiplicidad de derechos[15].

Con todo, en los diferentes planteamientos respecto de su contenido, podemos identificar que el elemento determinante para la evolución del derecho a la privacidad y la consiguiente configuración de un derecho a la autodeterminación informática es el desarrollo tecnológico, específicamente el desarrollo de las tecnologías de la información, que generaron un aumento en las capacidades para captar, tratar y transmitir la información[16]. Es tal esta preocupación que hoy en día podríamos hablar de una "cultura de protección de datos", que consistiría en esta creciente sensibilización hacia el valor que tiene la información personal, sensibilización que ha ido de la mano de un mayor conocimiento de los medios que los ordenamientos jurídicos disponen para la efectiva protección de los derechos de los titulares de datos[17].

Para cerrar este punto, son muy ilustrativas las palabras de Cerda, quien indica que "*podemos apreciar que la construcción del derecho a la autodeterminación informativa, o libertad informativa si se prefiere, sigue los derroteros propios de los derechos fundamentales de nueva generación: surgen a raíz de la 'liberties pollution' de las categorías precedentes, se abren paso tímidamente entre la doctrina y jurisprudencia nacionales, para finalmente cristalizar su reconocimiento en disposiciones legales, llegando a constitucionalizar su contenido e, incluso, a ser incorporados en instrumentos internacionales*"[18].

---

[14] En este sentido: MURILLO DE LA CUEVA, P. 1990. El Derecho a la Autodeterminación Informativa. La Protección de los Datos Personales frente a la Informática. Madrid, Editorial Tecnos. Citado en: CERDA, A. 2012. Legislación sobre protección de las personas frente al tratamiento de datos personales. *op. cit.*, 9p.

[15] ROSTIÓN, I. 2015. Sobre la Ley de Protección de la Vida Privada: La importancia de una "fuente legal" y su aplicación en las Personas Jurídicas. En: Revista Ius et Praxis 21(2): 501p.

[16] En este sentido, es muy decidor lo que indica el Tribunal Constitucional de España, en su sentencia 292/2000 de 30 de noviembre del año 2000, considerando cuarto, respecto de la necesidad de esta evolución del derecho a la privacidad ante el pujante desarrollo tecnológico determina que: *"Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, dado que una persona puede ignorar no solo cuáles son los datos que le conciernen que se hallan recogidos en un fichero sino también si han sido trasladados a otro y con qué finalidad, es suficiente indicar ambos extremos para comprender que* ***el derecho fundamental a la intimidad no aporte por sí solo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico****".*

[17] ZABALLOS, E., *op. cit*., 51p.

[18] CERDA, A., *op. cit.*, 10p.

En la actualidad, realizar esta precisión conceptual es mucho más importante en nuestro ordenamiento jurídico que en años anteriores, ya que en el mes de junio del año 2018 se publicó la reforma constitucional que consagra la protección de los datos personales[19], agregando una nueva frase en el numeral 4° del catálogo de garantías constitucionales. El texto indica que nuestra Carta Fundamental asegura a todas las personas "*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*"[20]. Hoy en día hay una diferenciación explícita de ambos derechos como categorías jurídicas separadas y no, como se realizó durante muchos años en la práctica de nuestros tribunales, utilizándose la afectación a la vida privada para deducir recursos de protección por tratamientos ilícitos de datos personales.

Volviendo a la ley en comento, siguiendo nuevamente a Cerda[21], nuestro legislador ha optado por una ley ómnibus, esto es, una normativa general aplicable en diversos contextos en los cuales se verifica un tratamiento de datos personales. La historia de la ley nos indica que los parlamentarios estimaban que esta regulación se constituía como una normativa marco, pues reglaría tanto los efectos del tratamiento de datos personales en la vida económica, como en otros ámbitos de la vida de las personas, como las relaciones laborales, prestaciones de salud, condenas o incluso podría funcionar como limitación al principio de transparencia pública. Así, podemos diferenciar con claridad la opción legislativa adoptada por nuestro legislador, distanciándose de un sistema sectorial, en que la protección de datos se regula distintivamente en base a la actividad de la que se trate, siendo ejemplo de ello la normativa estadounidense[22].

Finalmente, hay que destacar que esta "ley marco" procura alcanzar un equilibrio entre el legítimo interés que las personas tienen para reservar los datos que implican información concerniente a su persona y, por otro, el legítimo interés que tienen terceros de acceder a cierta información concerniente a éstos. En ese sentido, en su artículo 1° inciso 2°, se

[19] CHILE. Ministerio Secretaría General de la Presidencia. 2018. Ley 21.096: Consagra el derecho a protección de los datos personales. 16 de junio 2018.
[20] Anterior a la modificación, la carta fundamental se limitaba a indicar en este numeral lo siguiente: *"el respeto y protección a la vida privada y a la honra de la persona y su familia".*
[21] CERDA, A., *op. cit.*, 15p.
[22] En este sentido, en la legislación de Estados Unidos se dispersan las normas relativas a protección de datos según el sector de la actividad económica de la que se trate. Un ejemplo de esto lo tratamos en el apartado de derecho comparado del Capítulo III de este trabajo, en que diferenciamos en distintas leyes normativas relativas a seguridad de datos.

dispone 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 fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce*", es decir, establece explícitamente un derecho al tratamiento de datos, siempre y cuando se ejerza en base a los preceptos de la ley. Es una legislación que consagra en forma positiva la posibilidad del tratamiento de datos, reconociéndole a las personas naturales o jurídicas que pueden tratar datos, así como crear y mantener bancos o bases de datos, pero siempre observando las distintas disposiciones legales.

2. CONCEPTOS FUNDAMENTALES

Una vez indicadas las generalidades de esta legislación, pasaremos a revisar la terminología particular que nuestro legislador utiliza, especificada en el artículo 2° de la LPD, y que es importantísima a la hora de su aplicación.

2.1 DATOS PERSONALES

Para comenzar, el legislador en el artículo 2° letra f) define datos de carácter personal o datos personales como *los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.* Este es el concepto general más determinante en esta legislación, ya que es el núcleo de la protección de datos personales, siendo entendido por la doctrina como un concepto amplio[23] en el que quedan comprendidos variados antecedentes como el nombre, edad, sexo, estado civil, profesión, domicilio, números de teléfonos, entre muchos otros. En general, las leyes sobre protección de datos personales han definido a éstos en términos bastante amplios, entendiendo por tales a cualquier información respecto o concerniente a una persona a lo menos determinable. Esta amplitud del concepto permite cumplir con varios objetivos: facilita su adaptación a la constante evolución de la tecnología y la informática, utilizando el principio de neutralidad tecnológica; no limita el concepto solamente a información escrita, sino que también la imagen, la voz, las huellas digitales constituyen datos personales; y, el concepto admite "*hacer frente a uno de los peligros de la informática: la acumulación de datos personales y un ulterior cruce de los mismos; entrelazamiento que permite conocer, a partir de datos*

[23] ANGUITA, P. 2007. La protección de datos Personales y el derecho a la vida privada. Régimen Jurídico, Jurisprudencia y Derecho Comparado: análisis de la Ley No. 19.628 sobre Protección de la Vida Privada (Protección de Datos de Carácter Personal), modificada por la Ley No. 19.812. Santiago, Editorial Jurídica de Chile. p.295.

personales intrascendentes de una o varias personas, particularidades que pertenecen al ámbito protegido por el derecho a la intimidad"[24]. Cerda presenta de forma muy clara la idea detrás del concepto de dato personal, planteando que *dato* es una unidad básica de información, pero que, cuando la información que porta este dato se refiere a persona determinada o determinable, se denominará dato personal, esto es, una unidad de información que se predica de persona determinada o determinable[25].

A su vez, el legislador también realiza una categorización de los datos según el tipo de información que conllevan, de los que podemos identificar los siguientes: datos caducos, que son aquellos que han perdido su actualidad por determinadas situaciones; datos estadísticos, que son aquellos que en su origen o por consecuencia de su tratamiento, no pueden ser asociados a un titular identificado o identificable; datos sensibles, que son aquellos que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad[26]. En lo que respecta a esta diferenciación, se critica el tratamiento inorgánico que el legislador le da, ya que, si bien el artículo 2° de la LPD contiene las definiciones de los principales términos de la ley, únicamente precisa tres categorías particulares de datos, pero en otras disposiciones enuncia explícitamente otras categorías de datos personales, sin haberlas definido anteriormente y dándoles un tratamiento particular en base al tipo de información que conllevan.

Ejemplo de esta situación es lo que ocurre con la regulación de los datos relativos a obligaciones de carácter económico, financiero, bancario o comercial. Acá, el legislador plantea un título específico de la LPD para tratar su utilización, pero en ningún momento han sido definidos con precisión para saber cuándo estamos ante uno u otro tipo[27].

2.2 ÁMBITO MATERIAL DE APLICACIÓN

En lo que respecta al ámbito material de aplicación al que se ciñe la LPD, nos encontramos frente al tratamiento de datos personales, definido en el artículo 2° letra o)

[24] GRIMALT, P. 1999. La responsabilidad civil en el tratamiento automatizado de datos personales. Granada, Editorial Comares. 46p. Citado en: JERVIS, P., *op. cit*., 46p.
[25] CERDA, A., *op. cit.*, 16p.
[26] A mayor abundamiento, Jervis realiza una categorización en base a la mayor o menor exigencia de la autorización del titular como elemento que legitima el tratamiento de los datos. Véase: JERVIS, P. 2005. Categorías de datos reconocidas en la Ley 19.628. En: Revista Chilena de Derecho Informático(6): 111-145.
[27] Nos referimos al Título III "De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial", en el que se regulan aspectos como las condiciones de su tratamiento, situaciones de cesantía del titular o de protestos de letras de cambio y cheques, entre otras circunstancias, pero el legislador no entregó una definición en el artículo 2° de la LPD de estos tipos de datos.

como *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*. Nuestra legislación opta, nuevamente, por una terminología amplia, sin circunscribir el tratamiento de datos únicamente al realizado por medios automatizados, sino que considera tanto las formas de tratamiento automatizadas, como las manuales. De esta forma, la LPD "*se aplica a todos los tratamiento automatizados o manuales de datos personales que efectúen personas naturales o jurídicas, sean de carácter privado o público*"[28]. Esto cumple la finalidad de prever el mayor número posible de operaciones a las que puedan ser objeto de tratamiento los datos personales, dejando abierto el término al final de su definición. Con todo, la propia ley también se preocupa de definir algunas operaciones que conciernen al tratamiento de datos, como el almacenamiento, bloqueo, comunicación o transmisión, eliminación o cancelación, modificación y disociación de datos[29].

Al tratamiento de datos debemos entenderle como una serie de operaciones y procedimientos técnicos efectuados ya sea a través de medios automatizados o manuales, que permiten efectuar respecto de los datos personales una serie de acciones, por ejemplo, recogerlos, grabarlos, almacenarlos, conservarlos, elaborarlos, modificarlos, eliminarlos, bloquearlos, cederlos, comunicarlos, transmitirlos, transferirlos, etc[30]. A su respecto, cabe destacar que "*se trata de una serie de operaciones y procedimientos para realizar una serie de actos en los que se utilizan los datos de carácter personal y que, cada uno de ellos, constituye por sí mismo, una forma de tratamiento de datos*"[31].

---

[28] ANGUITA, P., *op. cit.*, p.291.

[29] A este respecto, en el artículo 2° podemos encontrar las siguientes definiciones:
a) Almacenamiento de datos, la conservación o custodia de datos en un registro o banco de datos.
b) Bloqueo de datos, la suspensión temporal de cualquier operación de tratamiento de los datos almacenados.
c) 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.
h) Eliminación o cancelación de datos, la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.
j) Modificación de datos, todo cambio en el contenido de los datos almacenados en registros o bancos de datos.
l) Procedimiento de disociación de datos, todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable.

[30] JERVIS, P. 2006. La regulación del mercado de datos personales en Chile. *op. cit.*, 51p.

[31] RUIZ, A. 1999. Los datos de carácter personal: concepto, requisitos de circulación, procedimientos, normativa y formularios. Barcelona, Bosch. 70p. Citado en: JERVIS, P., *loc. cit.*

Ahora bien, derivado del concepto de tratamiento de datos podemos evidenciar que en en esta operación pueden existir distintas etapas o momentos. En este sentido, Jervis ejemplifica que diversos autores, como Dávara indican que las etapas que se pueden reconocer son tres: a) la etapa de la toma, recolección o recogida de datos personales; b) la etapa del tratamiento de datos como tal; y, c) la etapa de comunicación o cesión de los datos a terceras personas diferentes de aquella que llevó a cabo el tratamiento. En este sentido, tal como nos señala el mencionado autor, estos tres momentos tienen incidencia al fijar los principios de la protección de datos, los derechos de los ciudadanos y los procedimientos que les permitan ejercer sus derechos[32]. En este sentido, Jervis nos destaca que esta distinción cobraría importancia por la forma diferenciada en que las leyes de protección de datos regulan las diversas etapas del procedimiento, estableciendo el cumplimiento de deberes, requisitos y principios diferentes[33].

Como mencionamos anteriormente, la LPD establece un derecho a tratar datos personales, explicitando tres aspectos que se deberán observar para el ejercicio legítimo de éste: i) el tratamiento debe hacerse de manera concordante con la LPD; ii) las finalidades del tratamiento deben ser permitidas por el ordenamiento jurídico; y iii) el tratamiento debe respetar el pleno ejercicio de los derechos fundamentales de los titulares de datos y de las facultades que la misma ley reconoce. En este sentido, la regla general y fundamental que se debe respetar como fuente de licitud del tratamiento de datos personales es la contenida en el artículo 4° inciso 1° de esta ley, que prescribe que *el tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consiente expresamente en ello*. No obstante, las principales excepciones a esta regla se encuentran en la propia LPD, que establece otras fuentes de licitud del tratamiento, teniendo entre las principales los datos provenientes de fuentes accesibles al público y el tratamiento efectuado por organismos públicos. Cabe destacar que la doctrina[34] ha observado con preocupación la forma en que se han tratado las excepciones, ya que el

[32] DÁVARA, M. A. 1997. Manual de Derecho Informático. Madrid, Editorial Aranzadi. 66p. Citado en: JERVIS, P., *op. cit.*, 51-52pp.

[33] JERVIS, P., *op. cit.*, 52p.

[34] Arrieta, siguiendo a Donoso y Reusser, considera que existen conceptos que generan dificultades interpretativas y que han servido para vulnerar la regulación, utilizando como ejemplo el concepto de fuente accesible al público que *"adolece de un defecto sustancial: radicar en el titular del registro o banco de datos la facultad de dejar o no abierto al público un registro, con el consecuente riesgo cierto de fraude al espíritu de la ley, especialmente en lo que dice relación con la posibilidad de realizar tratamiento de datos sin autorización del titular de los datos en aquellos casos en que la fuente es de esta naturaleza"*. Véase: ARRIETA, R 2009. Chile y la Protección de datos personales: Compromisos internacionales. En: Chile y la protección de datos personales: ¿Están en crisis nuestros derechos fundamentales? Serie de Políticas Públicas. Santiago, Ediciones Universidad Diego Portales. 19p.

legislador las desarrolló de tal forma que, en cierta medida, se haría que la autorización del titular fuese en la práctica la excepción y no la regla general.

Un ejemplo de lo anterior nos lo entrega Cerda[35]. con la disposición relativa a las fuentes accesibles al público y los datos que se recolectan de ellos. En este sentido, el artículo 4° de la LPD indica diferentes condiciones para usar datos captados de dichas fuentes sin el consentimiento del titular, como pueden ser que 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. Estas tres condiciones, ha aportado a que iniciativas privadas de generación de bases de datos para la búsqueda de personas según su cédula de identidad, o industrias como la del marketing directo (una de las más importantes a la hora de utilizar datos personales como un activo con valor económico y que maneja volúmenes de datos inmensos) pueda entablar comunicación entre prestadores de servicios y los posibles consumidores, pudiendo utilizar los datos de los últimos sin su consentimiento. A su respecto, la escueta regulación y delimitación de las fuentes accesibles al público, así como la amplitud de estas condiciones permite que se realicen numerosos tratamientos de datos en base a las excepciones que entrega la ley y no en base a la regla general.

2.2.1 PRINCIPIOS DEL TRATAMIENTO DE DATOS

El tratamiento de los datos personales está informado de una serie de principios sobre los que se funda la regulación, con tal de alcanzar el equilibrio de intereses que la ley propende. A modo de resumen tenemos los siguientes:

- Libertad en el tratamiento de los datos personales

Este principio está explicitado en el comienzo de la LPD y se condice con la idea de consagrar un derecho a tratar datos personales, de forma libre, pero siempre observando las disposiciones legales y los derechos fundamentales de los titulares.

En resumidas cuentas, el legislador consagra este principio de libertad en el tratamiento de datos personales, pero acto seguido condiciona su ejercicio a que se observen los siguientes aspectos: el tratamiento debe hacerse de manera concordante con la

[35] CERDA, A., *op. cit*., 21-22p.

LPD; las finalidades del tratamiento deben ser permitidas por el ordenamiento jurídico; y el tratamiento debe respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que la misma ley les reconoce[36].

- Información y consentimiento del titular

Como una de las finalidades de nuestra legislación es precisamente consagrar la protección a la autodeterminación informativa, es que se dispone que el tratamiento solo puede efectuarse cuando el titular consienta en ello. El legislador ha dispuesto que para que el consentimiento entregado sea válido, se debe informar debidamente al titular respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.

A la vez, la autorización reviste la solemnidad que debe constar por escrito para su validez, siendo esta revocable, pero sin efectos retroactivos[37].

- Finalidad en el tratamiento de datos

La LPD explicita que la autorización entregada se circunscribe a una determinada finalidad, excluyendo de licitud aquellos tratamientos que la excedan. La finalidad está muy ligada a la información que se le debe entregar al titular para que entregue su consentimiento, por cuanto acá se indica, explícitamente, para qué se están entregando los datos. Una forma común en que podemos observar una infracción a este principio ocurre en los casos en que entregamos nuestros datos para realizar una compra electrónica (por lo que su tratamiento se circunscribe únicamente a realizar esta operación), pero con posterioridad nos damos cuenta que comenzamos a recibir promociones comerciales al correo electrónico que entregamos en la compra, siendo que en ningún momento autorizamos que se utilizaran estos datos para que se nos perfilara comercialmente y se nos enviaran informaciones comerciales en forma directa.

A la vez, cabe tener presente que existe la Ley N°20.575[38], modificatoria de la LPD y que regula el principio de finalidad en el tratamiento de datos personales de carácter económico, financiero, bancario o comercial a los que se refiere el Título III de la LPD.

- Calidad de los datos

[36] CERDA, A., *op. cit.*, 20p.
[37] Artículo 4° incisos 3° y 4° de la LPD.
[38] CHILE. Ministerio de Economía, Fomento y Turismo. Ley 20.575: Establece el principio de finalidad en el tratamiento de datos. 17 de febrero 2012.

Este principio expresa dos ideas complementarias: por un lado, la información que se proporciona debe ser representación fiel de la realidad a la que se refiere; y, por otro, que éstos deben ser pertinentes y no excesivos en relación con el ámbito y objetivo para los cuales fueron recogidos.

Nuestra legislación ha acogido este principio en el primero de estos sentidos, exigiendo que la información personal se corresponda con la situación real del titular a quien conciernen, lo que importa que los datos sean veraces, exactos y actualizados[39].

- Protección especial de ciertas categorías de datos

Acá se hace referencia a la protección de los datos sensibles (ya definidos anteriormente en el trabajo), por cuanto suministran información particularmente importante y, por ende, su tratamiento ilícito es especialmente atentatorio contra los derechos de su titular. En este contexto, nuestro legislador estableció una regla especial respecto a la libertad de tratar datos, disponiendo que los datos de esta categoría no pueden ser objeto de tratamiento, salvo por tres excepciones: cuando la ley lo autorice; cuando exista consentimiento del titular; y cuando sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares. Con todo, la doctrina es crítica[40] respecto a la exigua e inorgánica regulación que la LPD le confiere a los datos sensibles, ya que únicamente se limita a establecer una regla de legitimación particular, pero no se aprecian a lo largo mayores especificaciones, como puede ser la diferenciación de las autorizaciones, ya que si una de sus fuentes de licitud es exactamente igual a la regla general del artículo 4°, no teniendo sentido establecer un estatuto de excepción en razón de la información especialmente sensible de estos datos.

- Seguridad de datos

Este principio es particularmente importante para este trabajo, por cuanto el deber de seguridad de los datos es expresión de él. Para efectos de esta parte del trabajo, nos limitaremos a indicar que éste hace referencia a la imposición que pesa sobre el responsable de proteger los datos que se encuentran en su poder.

---

[39] Artículo 9° inciso 2° LPD.

[40] En este sentido véase: CERDA, A., *op. cit.*, 25p.
De igual forma, es muy interesante el análisis sobre los datos sensibles presente en: GARRIDO, R. y BECKER, S. 2017. La biometría en Chile y sus riesgos. En: Revista Chilena de Derecho y Tecnología(6): 67-91.

Este principio se encuentra comprendido en el artículo 11° LPD que dispone que, con posterioridad a la captación de los datos, existe un deber de cuidarlos con la debida diligencia. En el tercer capítulo de este trabajo analizaremos específicamente este artículo.

- Deber de secreto

Finalmente, el deber de secreto alude a la reserva que se debe realizar del contenido de la información que ha sido objeto de tratamiento, recayendo tanto sobre el responsable, como sobre los trabajadores que intervienen en los distintos procesos en que se tratan datos. Se diferencia del principio de seguridad en tanto que el primero hace referencia al cuidado de la información personal en sí, mientras que el presente principio se juega respecto de las personas que trabajan en el tratamiento de datos y que supone la confidencialidad de la información a la que tuvieron acceso.

2.3 ÁMBITO SUBJETIVO DE APLICACIÓN

En lo que respecta al ámbito subjetivo de aplicación de la LPD, nos encontramos principalmente con dos figuras: titular de datos personales y responsable de datos personales.

- Titular de datos personales

La LPD en su artículo 2° letra ñ) dispone que el titular de datos es *la persona natural a la que se refieren los datos de carácter personal.* Si bien la definición pareciese ser explícita, la determinación de quién es el titular de datos ha presentado una serie de problemáticas, principalmente en la jurisprudencia, ya que en más de una ocasión se han aplicado las disposiciones de la LPD, en lo concerniente al titular de datos, respecto de personas jurídicas.

Ante esta disyuntiva, nuestra postura es que los titulares de datos son, exclusivamente, **las personas naturales**, excluyendo a las personas jurídicas de esta categoría. El legislador es claro en su definición y, por ende, como interpretes debemos atender a lo dispuesto en los artículos 19° y 20° del Código Civil (en adelante "CC"), no cabiendo la posibilidad de extender el concepto jurídico de "titular de datos" a las personas jurídicas, ya que explícitamente se nos indica que son únicamente las personas naturales, sin mencionar a aquellas en su definición. Del mismo modo, la doctrina y derecho comparados son contestes a la hora de establecer quién es el titular de datos, teniendo como ejemplo al Reglamento General de Datos de la Unión Europea, que de partida en los dos primeros

incisos de su artículo 1° precisa que: "*El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos*"*;* y "*el presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales*", respectivamente[41].

Es necesario tomar una postura clara ante esta situación, ya que nuestra Corte Suprema en variados fallos ha aplicado la normativa de datos personales respecto de las personas jurídicas como titulares. Por ejemplo, en la sentencia rol N° 961-2018[42], que resolvió la apelación de un recurso de protección deducido por una empresa al publicarse en el sistema de registro de morosidades de facturas anuladas y su inclusión en el predictor empresarial con mala calificación. En este fallo, no se expresó argumentación alguna para esbozar la aplicación de la normativa de la LPD a las personas jurídicas como titulares de datos personales, utilizándose directamente. A la vez, en otras sentencias en que se ha rechazado esta aplicación, se han presentado votos de minoría que indican que las personas jurídicas sí son tuteladas por la LPD. En sentido, tenemos el voto de minoría de una de las últimas sentencias de la Corte Suprema que se pronuncia respecto de esta problemática[43]. Acá la argumentación fue directa en indicar que la LPD incluye a las personas jurídicas en su protección, debiendo tomarse en consideración que no existe en esta ley alguna norma

[41] De igual forma, esta normativa de la Unión Europea indica explícitamente en su recital 14° que: *"La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.".* A lo largo de este trabajo, citaremos en varias ocasiones a esta normativa, por cuanto es el estándar ideal y más alto en materia de protección de datos del mundo.

[42] Corte Suprema, en sentencia de 23 de marzo de 2018. Rol N°961-2018.

[43] Corte Suprema, en sentencia de 16 de octubre de 2018. Rol N°12.617-2018. Acá nuestro máximo tribunal indicó lo siguiente en los dos primeros considerandos:
"*1.°) Que, como primera cuestión, las disposiciones de la Ley N°19.628 favorecen también a las personas jurídicas. En efecto, el artículo 4 de la mencionada ley señala las circunstancias en que puede realizarse una publicación, norma que constituye una disposición protectora de carácter general que debe inspirar la interpretación de la misma. Al respecto cabe consignar que no existe en esa disposición norma alguna que permita concluir que sólo es aplicable a personas naturales y que excluya de la protección dispensada a las personas jurídicas. Por ello no resulta aceptable la argumentación en contrario, pues implica admitir que las personas jurídicas, por el sólo hecho de ser tales, quedan en situación desmejorada respecto de la protección de sus derechos constitucionales.*
2.°) Que, además, de la completa lectura de la Ley N° 19.628 sobre Protección de la Vida Privada o Protección de Datos de Carácter Personal, no se divisa precepto alguno que excluya, de modo expreso, a las personas jurídicas como titulares de la protección que se concede por dicho cuerpo normativo al tratamiento de los datos personales. Lo anterior se ve reafirmado en cuanto en el Título II de la referida ley, denominado 'De los derechos de los titulares de datos', y más específicamente en sus artículos 12 y 13, se habla genéricamente de 'Toda persona' y de 'El derecho de las personas a la información'".

que permita concluir que sólo es aplicable a personas naturales y que excluya de su tutela a las personas jurídicas. A la vez, se arguye los enunciados amplios del legislador en la LPD, en el sentido de que no manifiesta de forma expresa la exclusión de las personas jurídicas, sujetándose de enunciados como el nombre del Título II "De los derechos de los titulares de datos", para fundamentar que no hay diferenciación. Debido a ello, para el sentenciador no resulta aceptable la argumentación en contrario, pues implica admitir que las personas jurídicas, por el sólo hecho de ser tales, quedarían en una situación desfavorecida respecto de la protección de sus derechos fundamentales.

Esta interpretación es del todo errónea ya que se desentiende de la disposición expresa en que se define titular de datos, desconociendo el espíritu y desarrollo histórico que ha tenido la protección de datos y que fue tomado en consideración por el legislador a la hora de adoptar la LPD. A su vez, de la historia fidedigna de la ley del ramo es posible desprender en variados pasajes[44], ya sea en su texto original como de sus modificaciones y discusión en sala, que este cuerpo legal se encuentra precisamente orientado a la protección de los datos personales, entendiéndose la noción de personal como perteneciente o relativa a la persona natural. En este sentido, es esta línea argumentativa la que adopta nuestro Máximo Tribunal[45] para resolver esta discusión, indicando en su argumentación,

[44] En este sentido, por ejemplo, véase: Historia de la Ley N°19.628. p. 96; p. 169; p.207; p.268. Disponible también en línea: <https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/6814/> [consulta: 21 de diciembre de 2018]

[45] Corte Suprema, en sentencia de 10 de mayo de 2018. Rol N°2204-2018. Acá el tribunal indicó que:
"*Cuarto: Que además, y en concordancia con las obligaciones impuestas por el artículo 1 de la Ley N°19.628, a quienes efectúen tratamiento de datos personales –entre los que destaca el "respeto por el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que la ley les reconoce"-, el artículo 2° del citado precepto, en su letra ñ), dispone expresa y claramente que: "Para los efectos de esta ley se entenderá por: ñ) Titular de datos, la persona natural a la que se refieren los datos de carácter personal".*
Quinto: Que, al margen de lo ya indicado, de la historia fidedigna de la ley en cuestión es posible desprender de varios de sus pasajes, ya sea de la moción del proyecto original, sus modificaciones y/o discusión en sala, que dicho cuerpo legal se encuentra orientado a la protección de datos personales, entendiendo la noción personal como perteneciente o relativa a la persona natural.
Es así como se señala en la moción de la ley que: 'De acuerdo a la doctrina expresada en los diversos instrumentos internacionales y textos constitucionales que se refieren a la materia, la vida privada de las personas pertenece a la categoría de los derechos humanos". *Agrega más adelante:* "*Partiendo del precepto contenido en el artículo 19 N° 4 de nuestra Carta Fundamental, nuestra moción comienza anunciando la inviolabilidad de la vida privada y advirtiendo que toda intromisión es, en principio, ilegítima. Se enuncian los principales aspectos a los que ella se extiende, tales como el derecho a la propia imagen; a la intimidad personal y familiar'. Y finalmente se señala en el Primer Informe de la Comisión de Constitución correspondiente al segundo trámite constitucional: 'Se aclaró que este artículo (artículo 2°) estaba referido a los datos personales de las personas naturales y se aplicaba en el ámbito de la intimidad. Por lo tanto, no es aplicable a las personas jurídicas'.*
Sexto: Que, tal y como ha dicho esta Corte en sentencia rol 4949-2012, en la normativa vigente no existe una regulación expresa en materia de remisión de información sobre personas jurídicas. Por ende, no existiendo norma legal que impida publicar o hacer circular una factura, ha de concluirse que, situado el conflicto en el ámbito del derecho privado en el que se puede realizar todo aquello que no está prohibido por la ley

precisamente, que tanto la definición que nos entrega el artículo 2° letra ñ) de la LPD, así como su historia fidedigna, nos entregan la pauta para delimitar que este cuerpo normativo está dirigido a tutelar a las personas naturales.

Compartimos esta argumentación, siendo a nuestro juicio el desarrollo histórico de la legislación de datos personales, la historia de la ley y la definición explícita que entrega el legislador, los argumentos para entender de forma inequívoca que el titular de datos personales es exclusivamente la persona natural, excluyendo de su protección a las personas jurídicas**.** De hecho, en su momento fueron presentados proyectos de ley[46], que no avanzaron en su tramitación y que tenían como objetivo explicitar la protección de la información de las personas jurídicas, incorporándolas al ámbito de aplicación de la LPD. De igual forma, existen legislaciones como la argentina[47] que explícitamente indican que las personas jurídicas también son titulares de datos personales, lo cual, si bien entendemos que sería una extensión errónea por parte del legislador trasandino, ya que desconoce los fundamentos de la protección de datos personales, nos parece correcta la formulación **expresa** que realiza al adoptar esta postura, explicitando el cambio en la figura del titular de datos.

Para nosotros, lo que se ha realizado en la Corte Suprema es una extensión incorrecta de la aplicación de la LPD en base a un criterio de justicia material, el cual alude a una suerte de situación de "indefensión" de las personas jurídicas para configurar una contravención legal que justifique la procedencia del recurso de protección, fundamentando la aplicación incorrecta del derecho en base al resguardo de garantías constitucionales.

A efectos de este trabajo es sumamente necesario el delimitar con claridad quién es el titular de datos personales, ya que cuando analicemos con posterioridad el régimen de responsabilidad civil y el deber de seguridad de datos, daremos cuenta de que el legitimario activo para interponer la acción es, precisamente, el titular de datos.

---

expresamente, la conducta de las recurridas no resulta contraria al ordenamiento jurídico, lo que desde luego, obsta a que la presente acción constitucional pueda prosperar".
Es particularmente interesante esta sentencia, por cuanto los ministros Aránguiz y Prado, en voto de minoría, presentaron una argumentación similar a la que anteriormente citamos en favor de que las disposiciones de la LPD son aplicables a las personas jurídicas.

[46] Por ejemplo, tenemos el Boletín N°2422-07 "Estable normas sobre protección de la información de las personas jurídica".

[47] Esta es la Ley N° 25.326, que indica expresamente en el inciso 2° de su artículo 1° que: "*Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal*".

De igual manera, esta claridad nos permite identificar quién es el beneficiado por una serie de derechos que consagra la ley y que puede ejercer en contra del responsable de datos, a saber: derecho de información o acceso a los datos; derecho de modificación, cancelación o bloqueo de los datos; derecho a la obtención de copia del registro de datos; y derecho de oposición, los que caracterizaremos sucintamente para una presentación más acabada de nuestra LPD:

i. Derecho de información o acceso: Este derecho supone "*tener la posibilidad de conocer la existencia de un determinado registro o banco de datos y la información que posee sobre una determinada persona*"[48]. En ese sentido, es amplio el abanico de objetivos específicos por los cuales se puede ejercer este derecho, pudiendo solicitarle al responsable la determinación del origen del dato, el contenido de la información personal, o incluso para saber si un banco de datos contiene o no información personal del titular.

ii. Derecho de modificación, cancelación o bloqueo: Estos derechos se ejercen bajo el supuesto de que los datos contenidos en el registro o banco de datos dejan de responder a la situación real que predican, o bien haya cesado la fuente de legitimidad de su tratamiento. Ante esta situación, el titular del dato tiene derecho a que su información sea modificada, eliminada o bloqueada. De forma sucinta diferenciaremos estos tres:

    - Modificación: Cuando exista un cambio en el contenido de los datos almacenados en el registro, se puede solicitar su rectificación[49], toda vez que estos resultan erróneos, inexactos, equívocos o incompletos. En ese sentido, el legislador al establecer las condiciones de utilización de datos personales, indica también que ellos han de ser modificados cuando concurra alguna de tales circunstancias[50], es decir, cada vez que los datos dejen de ser veraces y representen con exactitud aquello que predican respecto del titular.

[48] CORRAL, H. 2001. De los derechos de las personas sobre los responsables de bancos de datos: el hábeas data chileno. En: Cuadernos de Extensión Jurídica. Universidad de Los Andes(5). p.43
[49] Artículo 12° inciso 2 de la LPD.
[50] Artículo 6° inciso 2° de la LPD.

- Cancelación: Este derecho permite solicitar la destrucción o eliminación del dato que está en manos del responsable[51], toda vez que el tratamiento carece de fundamento legal (consentimiento del titular o autorización dada por el legislador) desde su captación, o también cuando el titular ha revocado la autorización para el tratamiento.

- Bloqueo: Este derecho supone que "*se faculta al titular para requerir la suspensión temporal de toda operación de tratamiento de los datos en cuestión*"[52]. A la vez, también procede en subsidio de su eliminación, cuando el titular revoque el consentimiento prestado para su procesamiento o no desee figurar en una base de datos empleada en comunicaciones comerciales, temporalmente. De ser definitivo, procede la eliminación de los datos[53]. Igualmente, el bloqueo de los datos opera cuando no sea posible establecer su exactitud o su vigencia sea dudosa y no corresponda la cancelación[54].

iii. Derecho a obtener copia: Cuando el titular ejerce el derecho de modificación o cancelación, la ley le reconoce además el derecho a obtener copia del registro alterado[55]. La obtención de esta copia es gratuita para el solicitante, pero para evitar abusos en el ejercicio de este derecho, una segunda solicitud de copia debe ser pagada, salvo que hayan transcurrido un plazo mínimo de seis meses entre la primera y la segunda petición.

iv. Derecho de oposición: Si bien se encuentra en un título aparte, Corral[56] destaca que la LPD en su artículo 3° inciso 2° consagra un derecho en favor del titular para oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión.

- Responsable de datos personales

[51] Artículo 2° letra h) de la LPD.
[52] CERDA, A., *op. cit.*, 29-30pp.
[53] Artículo 12 inciso 4° de la LPD.
[54] Artículo 6° inciso 3° de la LPD.
[55] Artículo 12° inciso 5° de la LPD.
[56] CORRAL, H., *op. cit.*, 46p.

Por contrario a la situación que se da con el titular de datos personales, la figura del responsable abarca tanto personas naturales como personas jurídicas. En específico, en el artículo° 2 letra n) de la LPD, se define responsable del registro o banco de datos como *la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal*. A la legislación le es indiferente el tipo de personalidad de quién realiza el tratamiento, puesto que su posición como responsable se verifica en base a las operaciones que realiza respecto de los datos personales que recoge. Con todo, la doctrina[57] ha sido crítica respecto a la definición del responsable, ya que haría falta clarificar con mayor precisión quién es. Si bien, la ley presenta definición, únicamente lo hace respecto del responsable del registro o banco de datos, mas no del responsable del tratamiento de éstos. Una cosa sería el conjunto organizado de datos personales y su respectivo responsable, y otra cuestión diferente es la situación en la que se encuentra el sujeto que toma las decisiones operativas respecto del banco de datos y en quien debiese recaer la responsabilidad por el uso ilícito de los datos personales.

En esta situación, si bien no existe una expresa diferenciación en las definiciones que nos da el legislador, en el artículo 8° trata el caso del tratamiento de datos en virtud de un mandato. Respecto de esto se dispone que se aplicarán las reglas generales de este tipo de contrato, por lo cual, el tratamiento se hará por cuenta y riesgo del mandante. De igual forma, en el inciso segundo de este artículo se indica que deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos.

Cabe destacar las reglas particulares que tienen los organismos públicos como responsables de datos, ya que el artículo 20° de la LPD indica explícitamente que *el tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular*. De esta forma, el tratamiento de datos por parte de organismos públicos es una excepción a la regla general del consentimiento del titular, pero únicamente se circunscribe a las competencias que por ley tendrá para tratar datos personales.

Finalmente es importante hacer mención a la inexistencia de autoridad de control de datos personales en nuestro país. En el ámbito comparado, para asegurar el debido

[57] ARRIETA, R., *op. cit.*, 20p.

cumplimiento de la normativa de datos personales se han establecido autoridades administrativas que sancionan las inobservancias a las disposiciones y que, además, procuran asegurar los derechos de los titulares. En ese sentido, lo más cercano a una autoridad de control en nuestro país podría ser el Consejo para la Transparencia, ya que, en sede de acceso a la información pública, procura resguardar los datos personales que se encuentren involucrados dentro de la información solicitada. Esto se dispone en el artículo 33° letra m) de la Ley N°20.285[58] Sobre Acceso a la Información Pública, que indica que entre las facultades y atribuciones de esta entidad se encuentra el velar por el adecuado cumplimiento de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado.

Planteados los aspectos generales de la protección de datos en nuestro país, procederemos a analizar en específico el régimen de responsabilidad civil regulado por la LPD y, posteriormente, la seguridad de datos personales.

[58] CHILE. Ministerio Secretaría General de la Presidencia. Ley 20.285: Sobre Acceso a la Información Pública. 20 de agosto 2008.

CAPÍTULO II: INDMENIZACIÓN DE PERJUICIOS DEL ARTÍCULO 23° DE LA LEY N°19.628

1. LA ACCIÓN DE INDMENIZACIÓN DE PERJUICIOS DEL ARTÍCULO 23°

En este capítulo analizaremos el régimen de responsabilidad civil regulado por la LPD que se encuentra en su Título V "De la responsabilidad por las infracciones a esta ley", el que contiene un único artículo que establece todo lo relativo a la indemnización de perjuicios por el tratamiento ilícito de datos personales, el cual reproduciremos íntegramente para pasar a su estudio pormenorizado:

> *Artículo 23.- La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.*
>
> *La acción consiguiente podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En todo caso, las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez. El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.*

1.1 GENERALIDADES

Desde sus orígenes como moción parlamentaria la ley tenía por propósito brindar protección a la vida privada de las personas en el ámbito del derecho civil, excluyendo la regulación de ilícitos de carácter penal. Específicamente, nuestra LPD al igual que otras legislaciones comparadas establece un régimen de responsabilidad civil que responde en

forma amplia[59] ante los daños derivados de un tratamiento ilícito de datos personales, debiendo responderse tanto por el daño patrimonial, como del daño moral provocado.

Como primer punto a tener en consideración es dejar en claro que la responsabilidad civil por tratamiento ilícito de datos personales que analizaremos es de carácter extracontractual y no contractual. La LPD regula en su artículo 23° un supuesto de responsabilidad extracontractual aún cuando podría parecer que, en los casos en que el titular otorgue expresamente y por escrito la autorización para el tratamiento de sus datos, se pueda dar lugar a un vínculo contractual. Esto resulta erróneo, toda vez que la autorización para tratar datos personales es un acto unilateral[60] y no necesariamente un acuerdo de voluntades del que emanarán derechos y obligaciones. Por lo demás, nuestra doctrina es conteste[61] al analizar el régimen de responsabilidad civil de la LPD, entendiendo que nos encontramos ante una regulación de orden extracontractual.

Ahora bien, existen posturas divergentes respecto del régimen de responsabilidad extracontractual al que se adscribe esta legislación, ya sea el régimen general de responsabilidad por culpa, o ya sea un régimen de responsabilidad objetiva o por riesgo. Pasaremos a exponer los argumentos brindados para cada una:

- Responsabilidad objetiva o por riesgo

Como defensor de esta postura tenemos a Cerda, quien indica que "*el legislador ha establecido un sistema de responsabilidad objetivo en la materia, que prescinde de la concurrencia de un elemento subjetivo en el agente y al cual basta la constatación de que el tratamiento se ha verificado indebidamente. Por lo demás, tal sistema es el que mejor se aviene con el propósito de salvaguardar los derechos del titular frente a los riesgos que importa el tratamiento de sus datos mediante el empleo de las nuevas tecnologías*"[62]. Respecto de esto, precisa que, a diferencia de lo que ocurre en otras legislaciones en que el criterio de responsabilidad está definido expresamente por la ley, en el caso de la LPD resulta de la interpretación legal, lo cual genera una interpretación disímil que es

[59] Por ejemplo, el artículo 82 del GDPR, titulado como "Derecho a indemnización y responsabilidad", en su inciso primero indica que: "*Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos*".
[60] Véase, por ejemplo: CORRAL, H., *op. cit.*, 54p.
[61] A este respecto Corral, Jervis, Cerda y Parada, en sus distintos trabajos citados en esta memoria, no cuestionan el carácter extracontractual de la responsabilidad por el tratamiento ilícito de datos personales. La discusión recae en el tipo de responsabilidad extracontractual que es regulada.
[62] CERDA, A., *op. cit.*, 40p.

rechazable. Posteriormente, para reforzar su planteamiento relativo a la procedencia de este estatuto de responsabilidad, nos entrega tres razones[63]:

i. El vocablo "indebido" utilizado en el artículo 23° denota un juicio de valoración normativo y no subjetivo;

ii. Carecería de sentido el tratamiento del tema en la ley si lo que se pretendiera fuese instaurar un régimen de responsabilidad subjetiva, ya que éste constituye la regla general en nuestro derecho; y

iii. El parámetro objetivo se adecua a las condiciones de la sociedad moderna, compleja y tecnologizada.

- Responsabilidad por culpa

En esta postura tenemos a Corral, quien indica que la ley se refiere a la responsabilidad civil como anexa a la responsabilidad infraccional, lo que sólo se condice con la responsabilidad civil extracontractual. De ello, en lo no previsto se aplicarán las normas de los artículos 2314° y siguientes del Código Civil. A su juicio, de la expresión perentoria "deberá indemnizar", alguien podría deducir que estamos ante un caso de responsabilidad objetiva, pero lo niega esgrimiendo las siguientes razones[64]:

i. El régimen común de la responsabilidad es el principio de la culpa, y para que haya excepción a este principio debe existir una norma inequívoca al respecto.

ii. La expresión "deberá indemnizar" no dice más que, cumplidos los presupuestos de la responsabilidad, nace la obligación de indemnizar.

iii. La responsabilidad civil en el artículo 23° aparece como anexa a la infracción legal, y ésta no puede existir sin negligencia o culpa. No hay responsabilidad contravencional sin dolo o culpa.

iv. La historia de la tramitación de la ley confirma esta conclusión, pues consta que se agregó el calificativo de "indebido" al tratamiento de datos que produce

[63] Íbid. Nota al pie.
[64] CORRAL, H., *op. cit.*, 54-55.

responsabilidad, justamente para enfatizar la necesidad de la aplicación de las reglas generales de la responsabilidad por culpa.

En lo que respecta a nuestra posición, compartimos la argumentación de Corral[65], adscribiendo a que el régimen de responsabilidad civil de la LPD es el sistema general por culpa de nuestro ordenamiento jurídico. Uno de los argumentos más fuertes para apoyar esta postura se encuentra en la historia de la ley, donde se indica que "*La Comisión Mixta estimó apropiada la sugerencia de ACTI de precisar que la indemnización de perjuicios que se consagra procederá cuando exista un tratamiento 'indebido' de los datos de una persona, **ya que ello despeja cualquier duda acerca de la aplicación de las reglas generales de responsabilidad extracontractual consagradas por el Código Civil***"[66]. A mayor abundamiento, esta opción se refuerza en que la jurisprudencia ha entendido de forma uniforme que estamos ante un régimen de responsabilidad por culpa, planteando, en juicios de indemnización de perjuicios por infracciones a la LPD, a modo de puntos de prueba los elementos que configuran nuestro régimen de responsabilidad por culpa[67].

A su vez, los planteamientos de Cerda sobre la presencia de un régimen de responsabilidad objetivo son criticables, principalmente porque desatiende la historia de la ley que permite precisar los objetivos que tenía el legislador, así como interpreta la realidad regulatoria desde un "deber ser". Esto último se grafica en que su argumentación se sustenta en lo que estaría más acorde o debiese ser más correcto para la efectiva protección de los titulares de datos y sus intereses, interpretando la ley en base al ideal que a su juicio debiese estar establecido. Y, a su vez, debemos tener presente que un sistema de responsabilidad civil de dichas características es excepcional, y por ello sus casos deben quedar explícitamente dispuestos por el legislador, no siendo procedente la construcción de sus casos en base a la interpretación doctrinaria.

1.2. PROCEDIMIENTO PARA SU TRAMITACIÓN

En adelante nos detendremos a analizar los aspectos procesales al ejercer la acción de indemnización de perjuicios en comento.

---

[65] Esta es la postura comúnmente seguida, teniendo entre quienes la apoyan a Jervis y a Parada, por ejemplo.

[66] Historia de la Ley N°19.628. p.266. Disponible también en línea: <https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/6814/> [consulta: 21 de diciembre 2018]

[67] A modo de ejemplo está la sentencia del 16° Juzgado Civil de Santiago, rol C-29221-2015, que revisaremos más adelante.

Como primer punto a destacar, el sujeto activo de esta acción es el titular de datos personales afectado por un tratamiento de sus datos con infracción de las disposiciones de la LPD. Por su parte, el sujeto pasivo es el responsable del registro o banco de datos, indicando expresamente nuestro legislador que puede ser la persona natural, jurídica o un organismo público, sin consagrar acciones civiles diversas dependiendo del tipo de responsable del que se trate.

Ahora bien, existen problemáticas respecto de la titularidad pasiva de la acción de indemnización de perjuicios en base a la figura del encargado del tratamiento de datos. Este sujeto es quien *a solicitud del responsable y bajo sus directrices se limitará a ejecutar operaciones de naturaleza técnica, vinculadas al tratamiento sobre las cuales no tiene ninguna disposición*[68]. Por ello, si cometiese un error durante su cometido y a raíz de él se causare un perjuicio al titular de datos, la demanda civil indemnizatoria deberá deducirse en contra del responsable y no del encargado. Acá debemos remitirnos a las reglas generales del mandato, aplicando las reglas del Código Civil, derivado del artículo 8° de la LPD.

En este mismo caso, siguiendo las reglas generales del mandato, el encargado deberá responder por los actos que generen algún tipo de daño a un titular de datos, cuando tales actos "*sean realizados fuera de las condiciones de utilización de los datos que han sido determinadas por el mandante y que la ley hace obligatorias de mencionar por escrito*"[69]. Por contrario, de actuar dentro de lo encargado, dentro de sus atribuciones y funciones, será el responsable del tratamiento quien tendrá la responsabilidad última de indemnizar los perjuicios provocados.

Ahora bien, también pueden existir problemas en este apartado en el caso particular del tratamiento de datos de carácter económico, financiero o bancario, ya que existen los registros de deudores que son de acceso público y que son llevados por corporaciones o personas jurídicas privadas. Por ejemplo, tenemos a DICOM. En este caso, si existiere una publicación en el boletín, sin fundamento legal, y se derivaren daños, en principio sería problemático para el titular saber contra quién accionará. No existe una regla especial al respecto, ni tampoco, necesariamente, la empresa que lleva el boletín es un encargado del tratamiento de datos y, por ende, no le son aplicables las reglas del mandato.

[68] PARADA, B. 2008. El régimen de responsabilidad civil en la protección de datos personales en Chile. Memoria de Licencia en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile, Facultad de Derecho. p. 88
[69] JERVIS, P., *op. cit.*, 158p.

Ante esta situación debemos dirigirnos a los términos generales y tener en consideración que el responsable del fichero es aquél que decide sobre las actuaciones concretas relativas al tratamiento de datos, con independencia del sujeto creador del banco o fichero de datos. Entendido esto, podemos identificar el elemento central para disuadir la situación si, en el caso accionamos contra el responsable o contra DICOM, siendo el poder de decisión del que está investido el responsable lo que nos permitirá distinguirlo de éste u otros sujetos que pudieren intervenir. Así, es el titular del dato, por ejemplo, un acreedor que tiene nuestros nombres, domicilio y detalles de una deuda, y que los informa a DICOM para que se mantengan en un registro público, siendo el primero el que tomó la decisión de comunicar el dato y quien desde un principio tiene el poder de decisión sobre los datos que originalmente captó[70] y que es, por tanto, el sujeto pasivo de la acción indemnizatoria ya que a él le es imputable el hecho de comunicar, de decidir sobre qué se realizará con el dato.

En cuanto a la competencia, la LPD no indica cuál es el tribunal llamado a conocer de esta acción, por lo que, al remitirse a las reglas generales, el tribunal competente es el Juez de Letras Civil del domicilio del responsable del banco o registro de datos. Tanto en la práctica judicial, como en la doctrina no ha existido discusión respecto a este aspecto no especificado por nuestro legislador[71].

En lo que respecta a las reglas del procedimiento, el artículo 23° indica que el juicio se sigue según las ritualidades de un procedimiento sumario. La excepción a esta forma de tramitación se da en los casos en que nos encontramos ante infracciones de los artículos 16° y 19° de la LPD, en los cuales se aplicaría un procedimiento diverso. Esto se debe a que, en estos preceptos, el legislador regula la negativa del responsable sobre lo solicitado por el titular de datos en virtud del ejercicio de sus derechos de reclamación, información, cancelación o bloqueo.

El legislador permite interponer la acción de indemnización de perjuicios conjuntamente a la reclamación destinada a declarar la infracción, por lo que, en el mismo

[70] Con todo, esto no quita que el responsable de un fichero de las características de DICOM esté exento de responsabilidades. Así, por ejemplo, se puede ejercer el derecho de acceso y de copia de nuestros datos que se encuentren en su poder, los cuales deberán ser respetados. Ante la negativa, podría ejercerse una acción de *habeas data*.

[71] Todos los juicios revisados en que se ejerce esta acción de indemnización de perjuicios no han terminado con la declaración de incompetencia del Juez de Letras Civil del domicilio del responsable de datos. De igual forma, autores como Cerda, Corral o Jervis, en sus diversos trabajos sobre la materia, no han cuestionado ni problematizado esta omisión.

juicio, el actor puede conseguir tanto una indemnización, como la multa a beneficio fiscal en contra del responsable infractor. A la vez, la ley indica que este proceder es sin perjuicio de que el tribunal puede reservar a las partes el derecho a discutir sobre el monto en la ejecución del fallo o en un juicio distinto[72].

Finalmente, el legislador mandata al juez a que tome todas las providencias que a su juicio sean necesarias para hacer efectiva la protección de los derechos que la LPD consagra.

1.3 HABEAS DATA

Para un análisis más acabado del artículo 23°, es necesario hacer alusión a la acción de *habeas data*, ya que el procedimiento diferenciado al que hace referencia dicho artículo es el seguido en el ejercicio de esta acción. Es decir, en caso de que nos encontremos con infracciones a los artículos 16° y 19° de la LPD, el procedimiento a seguir será distinto, por cuanto se tratará de un *habeas data*.

La LPD establece dos acciones de reparación para subsanar o prevenir daños que se podrían producir por un tratamiento de datos con infracción a la ley. Una es la que busca una reparación por equivalencia, que es la acción de indemnización de perjuicios del artículo 23° de forma autónoma. Por su parte, la acción de *habeas data* se condice con una reparación en naturaleza, ya que busca el amparo de los derechos consagrados en favor del titular de datos en la LPD, permitiendo solicitar la eliminación, modificación o bloqueo de sus datos. Se trata de una acción judicial específica y autónoma, de objeto definido y de tramitación concentrada, en virtud de la cual los titulares de datos "*pueden ver protegidos sus derechos frente a acciones que resulten ilegales o arbitrarias o que importen un uso indebido de información de carácter personal que le concierne por parte del responsable del fichero o banco de datos*"[73]. Busca un amparo directo y efectivo de los derechos del titular, siendo entendido el *habeas data* a la autodeterminación informativa como lo que el *habeas corpus* sería a la libertad personal[74].

De acuerdo con el artículo 16° de la LPD, el *habeas data* procede en los siguientes supuestos:

---

[72] Artículo 173° del Código de Procedimiento Civil.
[73] JERVIS, P. 2003. Derechos del titular de Datos y Habeas Data en la Ley 19628. En: Revista Chilena de Derecho Informático(2), Facultad de Derecho de la Universidad de Chile. p. 27
[74] PÉREZ-LUÑO, A. 1996. Manual de Informática y Derecho. Madrid, Editorial Ariel S.A., 44p. Citado en: CERDA, A., *op. cit.*, 38p.

i. Si el responsable del banco de datos no se pronuncia sobre la solicitud de información, modificación, bloqueo, cancelación o eliminación de datos del requirente dentro de los dos días hábiles que establece la ley.

ii. Si el responsable deniega la solicitud información, modificación, bloqueo, cancelación o eliminación de datos del requirente. En este caso el procedimiento a seguir será especial si la causal invocada para la denegación es la seguridad de la Nación y el Interés Nacional, siendo el tribunal competente para conocer del asunto la Corte Suprema.

En cuanto a la legitimación activa, la LPD indica que el ejercicio de esta acción le corresponde al titular de datos. A nuestro parecer, esta afirmación es restrictiva y compartimos las afirmaciones de Corral, en el sentido de que el artículo 16° tiene una interpretación más amplia, ya que, tratándose del derecho de acceso o información, la acción de *habeas data* podrá ser interpuesta por cualquier persona que tema estar incluida en alguna base de datos personales. Esto es debido a que nuestro legislador al referirse a los derechos de los titulares de datos en el artículo 12°, en su inciso primero señala que "toda persona" puede ejercer estos derechos, ya que no sería necesario demostrar que existe un dato del cual se es titular. Precisamente, el ejercicio del derecho de acceso consiste en la posibilidad que tiene una persona de *indagar sobre la existencia de información suya registrada*[75], independiente de que la gestión concluya con una respuesta afirmativa o negativa. A su vez, de ello derivamos que el ejercicio del resto derechos (modificación, bloqueo o cancelación, así como copia y oposición) corresponden exclusivamente a quienes efectivamente sean los titulares de los datos.

Respecto a la legitimación pasiva, la acción debe interponerse en contra del responsable del registro o banco de datos, independiente de que sea persona natural, jurídica u organismo público.

En cuanto a lo procedimental, por regla general[76] la acción se presenta ante el Juez de Letras Civil del domicilio del responsable del registro o banco de datos[77]. La reclamación

[75] CORRAL, H., *op. cit.*, 46-47pp.

[76] Tal como hicimos alusión anteriormente, existe un procedimiento especial que ocurre en casos que se deniegue la solicitud del titular invocando la seguridad de la Nación o el interés nacional. En estos casos se interpone la acción ante la Corte Suprema, la cual pedirá informe al responsable del modo más expedito posible y fijará su respectivo plazo. Vencido, pasará a resolver el asunto en cuenta. Si se recibe la causa a prueba, ésta debe consignarse en cuaderno separado y reservado. Finalmente, la Corte Suprema puede, de

deberá señalar la infracción cometida y los hechos que la configuran. A la vez, deberá ser acompañada de los medios de prueba que la acrediten, en su caso. Esta última expresión, "en su caso", nos lleva a la conclusión que este requisito no es de carácter perentorio[78] y que dependerá de la naturaleza de la infracción el que existan medios de prueba que efectivamente puedan ser acompañados a la reclamación.

La reclamación ejercida se notifica por cédula en el domicilio del responsable de datos, teniendo como plazo para contestar cinco días hábiles desde tal notificación. Dicha contestación es por escrito y a ella deben acompañarse los medios de prueba que acrediten los hechos en los que se funda. Si no dispusiese de estos medios en dicho momento, deberá indicar en esta contestación tal circunstancia y el juez fijará una audiencia dentro de quinto día hábil a fin de recibir la prueba ofrecida y no acompañada.

La sentencia definitiva deberá ser dictada dentro de tercer día hábil de vencido el plazo para contestar, se hayan presentado o no descargos, o desde que vence el plazo fijado en la audiencia a la que nos referimos en el párrafo anterior. Esta sentencia, de acoger lo solicitado, fijará un plazo prudencial para que el responsable de datos dé cumplimiento a lo resuelto. Se notifica por cédula, procediendo en su contra el recurso de apelación en ambos efectos, el cual deberá ser interpuesto dentro de quinto día hábil desde la notificación de la parte que entabla el recurso. Se siguen las mismas reglas comunes para el escrito de un recurso de apelación, debiendo contener los fundamentos de hecho y de derecho en que se basa, así como las peticiones concretas. La LPD agrega que el presidente de la Corte de Apelaciones respectiva deberá ordenar dar cuenta preferente del recurso, sin esperar comparecencia de las partes. Finalmente, ante la sentencia de segunda instancia no proceden recursos, salvo el recurso de queja al aplicar el artículo 545° del Código Orgánico de Tribunales.

En síntesis, la acción de *habeas data* tiene como finalidad la tutela de derechos consagrados en la LPD y se diferencia de la acción de indemnización de perjuicios

---

estimarlo conveniente o si le es solicitado con fundamento plausible, ordenar traer los autos en relación, caso en el cual la causa se agrega extraordinariamente a la tabla, debiendo disponer el presidente de la Corte Suprema que la audiencia no será pública.

[77] Cabe destacar que, durante la tramitación de la LPD, desde sus orígenes se discutió la posibilidad de que fuese competente el tribunal del domicilio del afectado. Esto entendido en base a la naturaleza de los derechos tutelados. No obstante, finalmente primó la postura de que se seguirán las reglas generales de competencia. Para más información: Historia de la Ley N°19.628. p. 6. [en línea: <https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/6814/> [consulta: 21 de diciembre de 2018]

[78] CORRAL, H., *op. cit.*, 52p.

consagrada en el artículo 23° en los casos en que no nos encontremos con las infracciones de los artículos 16° y 19° de la LPD, en cuya infracción lo normal será interponer conjuntamente ambas acciones o utilizar el *habeas data* como antecedente de una futura indemnización de perjuicios.

En el análisis específico que busca este trabajo, no nos centraremos en el *habeas data* como un antecedente de la acción de indemnización de perjuicio del artículo 23°, sino que nos enfocaremos en las vulneraciones o accesos a datos personales que no fueron resguardados con la debida diligencia y que supongan una violación al artículo 11° de la LPD.

1.4 TUTELA SUMARIA Y PARTICULARIDADES DE LA APRECIACIÓN JUDICIAL

Existen dos aspectos más a los que nos gustaría hacer referencia en el análisis del régimen de responsabilidad civil de la LPD, los cuales se encuentran muy ligados por los efectos prácticos que tienen sobre la decisión final del litigio.

Los aspectos a los que aludimos son el procedimiento sumario y la apreciación en conciencia del juez. Creemos que es particularmente valorable que se elige la opción sumaria para el procedimiento de indemnización de perjuicios por infracciones a la LPD, ya que se condice con el espíritu de los derechos tutelados. Tal como hicimos alusión en el primer capítulo de este trabajo, la evolución del derecho a la privacidad que dio paso a la creación de sistemas de protección de datos y un derecho a la protección de éstos, se basa en el avance de las tecnologías de la información y la comunicación, que se encuentran en todos los aspectos de nuestra vida hoy en día. En este sentido, la LPD es expresión regulatoria en el ámbito civil del derecho fundamental a la autodeterminación informativa, hoy en día consagrado en nuestra Constitución al garantizar la protección de los datos personales. Así, podemos afirmar que los derechos y sus posibles afectaciones que regula la LPD, tienen un prisma más sensible o con un valor que excede del ámbito netamente privado.

Ahora bien, de la lectura de la historia de la ley no se desprende explícitamente el por qué nuestro legislador optó por un procedimiento sumario para esta ley. Pero sí podemos llegar a ciertas conclusiones desde la interpretación de su tramitación.

Ya desde sus inicios como proyecto de ley, la LPD consagraba que la acción indemnizatoria y las restantes acciones de protección contempladas se sujetarían al procedimiento sumario[79]. Si recordamos que en un primer momento esta ley estaba pensada como una ley de protección de la vida privada en el ámbito civil, en que uno de sus aspectos era la protección de datos personales, lo que podemos concluir es que siempre se resguardo el derecho fundamental a la privacidad desde sus inicios. Si entendemos que la protección de derechos fundamentales requiere mayor celeridad, es que nos hace sentido que desde siempre se contempló proceder sumariamente para las acciones que regula esta ley.

Si bien, el legislador no justifica la utilización de un procedimiento sumario, desde la doctrina podemos indagar en los fundamentos que esta técnica procedimental tiene. En este sentido, Pérez indica que "*con la voz 'sumario' en Latinoamérica se alude a diferentes modalidades para la gestión de la variable y riesgo de la duración del proceso*"[80]. Con esto, desprendemos que en el caso de la LPD con la utilización de un procedimiento sumario se busca gestionar el tiempo en el proceso, ya que es un riesgo existente para ciertos derechos que, por su naturaleza, deben ser tutelados de la manera más pronta posible. Esta idea se refuerza si entendemos a lo sumario como una "*reacción directa contra el mito del procedimiento ordinario (declarativo o de conocimiento) tradicionalmente rígido y justificado en los argumentos de un tratamiento igualitario y de una previsión normativa general de la legalidad*"[81]. Un juicio ordinario de lato conocimiento es garantía, *prima facie*, de un justo y racional procedimiento, con rigidez y formalismos que prometen predictibilidad y un trato igualitario, pero también puede operar como una frustración de sus fundamentos, ya que en la práctica no logra adecuarse a las particularidades de determinados derechos y controversias, sin darles una solución óptima.

Ahora bien, esta es una interpretación ideal y que nuestro juicio es la que se sigue lógicamente de la naturaleza de la LPD, pero la utilización de la técnica sumaria no se da únicamente para tutelar derechos según su naturaleza, sino también por cuestiones de economía procesal del sistema. Lo sumario puede hacer referencia a una simplificación, abreviación y ambas, para llegar más rápidamente a una decisión, que se justifica en base a

[79] Historia de la Ley N°19.628. 6p. [en línea] <https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/6814/> [consulta: 21 de diciembre de 2018]
[80] PÉREZ, A. 2017. Tutela sumaria de derechos en el proceso civil: misión y visión en Latinoamérica. En: Revista Chilena de Derecho Privado(28). 137p.
[81] *Ibid.*, 141p.

la simplicidad de una controversia. Así, nuestro legislador podría haber previsto un procedimiento sumario ya que, a su juicio, las controversias no serían lo suficientemente difíciles o no requerirían de un procedimiento de lato conocimiento para su solución.

Relacionamos esta indagación con la apreciación judicial que establece el artículo 23° de la LPD, que indica que el juez apreciará la prueba en conciencia y que el monto de la indemnización será establecido prudencialmente, considerando las circunstancias y la gravedad de los hechos. A la vez, en el juicio, el juez podrá tomar todas las providencias que estime necesarios para hacer efectiva la protección de los derechos consagrados por la LPD. Acá, si interpretamos en su conjunto la norma, se recalca la idea de protección de derechos y que a nuestro juicio es la opción correcta a la hora de entender por qué nuestro legislador optó por una tramitación sumaria.

De existir futuras modificaciones legislativas respecto al marco regulatorio de la protección de datos, creemos que la opción sumaria y la apreciación de la prueba a conciencia son de las mayores virtudes que la actual LPD tiene, las cuales debiesen de conservarse a lo largo del tiempo. Esto ya que responden a los fundamentos de la protección de datos en tanto que derecho fundamental y, como tal, requiere de una protección más acelerada y con una valoración probatoria más laxa.

De igual modo, la apreciación de la prueba a conciencia y la delimitación prudencial de la indemnización permiten que el juez pueda anteponerse a una gran variabilidad de casos y, nuevamente, se condice con el espíritu de la protección de los datos personales. Si el juez se basa en su prudencia, podrá abordar con mucha mayor facilidad los avances de las tecnologías de la información, así como las diferentes formas en que se podría configurar la relación entre titular y responsable de datos.

1.5 REQUISITOS DE LA RESPONSABILIDAD CIVIL EN LA PROTECCIÓN DE DATOS

Una vez revisados los aspectos procedimentales del ejercicio de la acción consagrada en el artículo 23° LPD y la acción de *habeas data*, a continuación, realizaremos un breve análisis de los requisitos constitutivos de la responsabilidad civil y que nos permitirán verificar la procedencia de la indemnización de perjuicios.

- Acción u Omisión

Como es de común conocimiento, no existe propiamente responsabilidad si no existe un daño reconducible a la conducta libre de un sujeto. La LPD no realiza un tratamiento distintivo respecto de si es necesaria una acción o una omisión, siendo tanto el hecho positivo, como el negativo, posibles de generar responsabilidad en los términos del artículo 23°. A su vez, este hecho debe de ser imputable al sujeto, por lo cual debe ser ejecutado por alguien con capacidad delictual. En este sentido, no generan problemas las reglas de la capacidad en cuanto al tratamiento de datos realizados por personas jurídicas y organismos públicos, que son casi la totalidad de quienes tratan datos personales y que son, por ende, responsables de un registro o banco de datos. Ahora bien, si hipotéticamente hablando, quien realizara un tratamiento ilícito que genere daños sea un incapaz, ante el silencio de la LPD en este aspecto específico, se seguirán las reglas generales del derecho común[82].

Si analizamos los preceptos de la LPD, podremos dar cuenta que existen diversos hechos o formas de actuar que nuestro legislador trata, de una u otra forma, y que en la práctica podrían constituirse, valga la redundancia, como el hecho imputable del juicio de responsabilidad.

La principal directriz que tenemos para verificar lo anterior es la definición de tratamiento de datos que se realiza en la letra o) del artículo 2° de la LPD, ya que se indica que el tratamiento consiste en cualquier operación o complejo de operaciones, tanto automatizados como no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos o utilizarlos de cualquier otra forma. En este punto, el legislador manifiesta cuáles acciones conllevarían tratamiento de datos y que son las que con normalidad vendrían a la mente a la hora de pensar en la utilización de la información personal. Pero el legislador cierra la definición con una amplísima apertura de qué se puede entender por tratamiento de datos, permitiendo su concreción en una gran variedad de acciones.

Lo primordial de esta acción u omisión es que sea con infracción a las disposiciones de la LPD. En este sentido, el ejemplo más común de responsabilidad será el tratamiento ilícito de datos, el cual se verifica si no se cumple alguno de los siguientes supuestos:

i. Si el titular de los datos personales autorizó expresamente el tratamiento.

[82] En la jurisprudencia revisada para el desarrollo de esta investigación, no se han identificado casos en que ocurran estos hechos.

ii. Si la ley faculta al responsable para realizar tratamiento sin tener como base de legalidad el consentimiento, como podría ser captar el dato desde una fuente accesible al público.

Fuera de estas hipótesis, el tratamiento de datos infringe la regla de licitud del tratamiento y, por ende, es un tratamiento del que, de derivar daños, se podría exigir indemnización.

Ahora bien, también el hecho imputable puede ser la denegación del ejercicio de un derecho o la no respuesta ante la solicitud del ejercicio de derechos de un titular. En este sentido, nos remitidos a lo expuesto en el apartado en que tratamos el *habeas data*.

En síntesis, el hecho imputable para que proceda la responsabilidad por infracción a las disposiciones de la LPD es, por antonomasia, el tratamiento ilícito de datos. A la vez, existen otros supuestos como pueden ser la inobservancia del deber de seguridad o la no respuesta o denegación sin fundamento de la solicitud en que se ejerce algún derecho por parte del titular, siendo el primero de estos ejemplos tratado latamente en el próximo capítulo.

- Culpa o Dolo

Tal como lo indicamos al comienzo de este capítulo, la responsabilidad por contravención a las disposiciones de la LPD se adscribe al sistema general de responsabilidad por culpa, no obstante, existan argumentos que, en base a un ideal regulatorio, promuevan que se entienda como una responsabilidad objetiva o por riesgo, como es lo propuesto por Cerda. Además, es incorrecto aludir a ello toda vez que se tiene que tener presente que una característica primordial de un sistema de responsabilidad civil objetivo es su excepcionalidad, y por ello sus casos deben quedar explícitamente dispuestos por el legislador, no siendo procedente la construcción de sus casos en base a la interpretación que vaya ofreciendo la doctrina.

- Daño

El artículo 23° de la LPD prescribe que se indemniza tanto el daño moral como el patrimonial. Del análisis de los casos que hemos revisado para este trabajo, la más común problemática por la que se ejerce la acción de indemnización de perjuicios de la LPD deriva de la publicación, sin fundamento, de deudas en un registro de deudores y morosos,

como sería el caso de DICOM. En ese sentido, generalmente lo solicitado es indemnización por la imagen de insolvencia que adquiere la persona y la aflicción psicológica derivada de ello. Si de esa publicación se siguió causalmente la imposibilidad de negocios, crédito o pérdidas pecuniarias concretas, se solicita daño emergente y/o lucro cesante, no debiendo verificarse problemas generales a su respecto.

- Causalidad

A nuestro análisis de la LPD no aparecen problemas respecto a la relación de causalidad entre tratamiento ilícito de datos y el daño. Únicamente puede surgir la problemática práctica, respecto de la prueba de la causalidad, en el sentido de que, en casos de tratamientos automatizados o muy complejos, con el empleo de diversas tecnologías o procedimientos variados que estén a lo largo del tratamiento, pueden suscitar problemas probatorios para el titular.

2. ANÁLISIS COMPARADO

Para mayor exhaustividad, haremos una referencia breve al tratamiento que la legislación comparada realiza de la indemnización de perjuicios por el tratamiento ilícito de datos personales. Para ello, tomaremos dos países latinoamericanos, y principal estándar actual de tratamiento de datos que es la Unión Europea.

- Argentina

La ley que regula la protección de datos personales es la Ley N° 25.326, del año 2000. En su artículo 31° menciona que los responsables de datos están sujetos a la responsabilidad por daños y perjuicios derivados de la inobservancia de las disposiciones que establece, no lo consagra de forma expresa que los titulares tienen derecho a solicitar ante los tribunales una indemnización, por lo que al final, para cualquier reclamo de esta índole el titular deberá remitirse a las reglas generales del derecho civil.

Es una situación algo similar con la acontecida en nuestro país, con la diferencia de que en Argentina es más escueta la ley, no existiendo ninguna alusión al procedimiento a seguirse ni a la apreciación de la prueba rendida en dicho juicio.

- México

En cuanto a México, la ley que regula la protección de datos es la Ley Federal de Protección de Datos Personales en Posesión de Particulares, que data del año 2010. El

artículo 58° se prescribe la posibilidad de accionar por indemnización de perjuicios en caso de que el titular considerare que ha sufrido daño o lesión en sus bienes o derechos como consecuencia del incumplimiento a lo dispuesto en la ley por el responsable o encargado. Nuevamente no se hace alusión a reglas particulares de procedimiento, por lo cual hay que remitirse a las reglas generales de procedimiento civil.

Con todo, acá el régimen infraccionario está muchísimo más detallado que en el caso chileno o argentino, disponiendo en su artículo 63° cerca de una veintena de casos que se considerarán como infracciones a la ley. Aún más, la enumeración la cierra indicando que constituirá infracción "*cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la presente Ley*"[83]. A nuestro parecer es realmente útil esta enumeración, por cuanto permite esclarecer de forma no taxativa las infracciones a la ley de datos, concentrándolas principalmente en un artículo y no dejándolas, como en nuestro ordenamiento, de forma inorgánica y no siempre explicitada.

- Unión Europea

Sin lugar a duda el tratamiento de datos a nivel mundial tiene un antes y un después luego de la entrada en vigor del Reglamento General de Protección de Datos de la Unión Europea (GDPR, por sus siglas en inglés), en mayo de 2018. Principalmente, porque es el más alto estándar de protección de datos, estandarizando los derechos de los titulares y las obligaciones de los responsables en todos los Estados miembros de la Unión Europea. Pero, no únicamente eso, sino que tiene un régimen sancionatorio rígido, con exigencias estrictas y que pueden conllevar multas que pueden alcanzar el 4% del volumen de ingreso anual del responsable de datos, o 20 millones de euros, el que sea mayor.

Estas grandes multas generan todavía más impacto en las relaciones de las grandes corporaciones con los Estados de la Unión Europea, por cuanto el GDPR tiene pretensiones de aplicación extraterritorial[84].

---

[83] Artículo 63° numeral XIX.

[84] Su artículo 3° "Ámbito Territorial" indica que:

1.El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, ***independientemente de que el tratamiento tenga lugar en la Unión o no****.*

2.El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o ***encargado no establecido en la Unión****, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.*

En cuanto a la regulación de la responsabilidad civil, el artículo 82° "Derecho a indemnización y responsabilidad" indica que toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción al GDPR, tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

De igual forma, en el mismo artículo, este reglamento se antepone a la situación de operaciones complejas de tratamiento de datos, en que intervienen muchos responsables y/o encargados, estableciendo una forma de responsabilidad solidaria, al indicar que cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado[85].

Hoy en día el modelo de protección de datos del GDPR es tal referente que otras legislaciones han ido adoptando o buscando asimilar su normativa a los estándares de este reglamento general europeo. Ejemplo de ello es el actual proyecto de ley de protección de datos personales que discute en el Senado (N° 11.144-07 y 11.092-07, refundidos) que pretende mejorar el marco regulatorio de los datos personales en nuestro país y que en su texto original, como en las actuales indicaciones presentadas, se va perfilando una verdadera búsqueda por llegar al estándar europeo[86].

3. CRÍTICAS GENERALES

Para cerrar este capítulo, plantearemos nuestras críticas generales en contra del régimen de responsabilidad civil que actualmente se encuentra establecido en la LPD.

Tal como indica Parada, *"en lo que respecta a la protección de datos personales, el problema que más aqueja a las víctimas es el 'probatorio', porque en un régimen de responsabilidad por culpa es ella quien debe acreditar que el perjuicio sufrido debido a la imprudencia del autor*"[87]. Por lo general, la persona afectada será una persona natural que

---

3.El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que ***no esté establecido en la Unión*** *sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público.*

[85] Artículo 82° GDPR, inciso tercero.

[86] Ejemplo de ello son las diferentes categorías especiales de datos que se incluyen, como los relativos a niños, niñas y adolescentes, o datos genéticos y o biométricos, para colocar algunos ejemplos.
De igual forma, entre las indicaciones presentadas por el actual gobierno de Sebastián Piñera, se encuentra la búsqueda de aplicación de la LPD en casos en los cuales el responsable o el encargado y los titulares de los datos residen en Chile, independientemente de que el tratamiento tenga o no lugar en Chile, siendo muy similar a las pretensiones de extraterritorialidad del GDPR.

[87] PARADA, B. *op. cit.*, 81p.

no dispone de los medios económicos suficientes para enfrentarse en contra de las grandes empresas que funcionan en base al tratamiento de datos personales.

En añadidura y en directa relación con lo anterior, existe el problema general del poco control que tienen los titulares sobre su información. Si bien, existen una serie de derechos y un régimen de licitud del tratamiento, en la práctica la poca especificidad y orgánica con que la LPD trata materias como tratamiento transfronterizo de datos, tratamiento de datos sensibles, deberes de información del uso de los datos, entre otras, hacen que el titular tenga muy poco conocimiento de cuándo, cómo y dónde están siendo tratados sus datos. Existe una enorme diferencia entre titular y responsable en cuanto a la posibilidad de probar los hechos del tratamiento, ya que en la actualidad los derechos del responsable entran a ejercerse *ex-post* una infracción a la LPD. Un ejemplo práctico de esto es ejercer el derecho de cancelación respecto de un dato que el titular descubrió que fue publicado en un determinado fichero que no se encontraba en manos de la persona a la que le autorizó a tratar datos. La problemática radica en que para el titular es prácticamente imposible probar que existió una cesión de alguna base de datos desde un determinado responsable a otro, ya que no hay, hoy en día, un efectivo seguimiento de la "vida" del dato o de la trayectoria de su tratamiento.

Este problema podría ser solucionado, por ejemplo, si existiese efectivamente la obligación de registrar las bases de datos creadas por privados y que los titulares pudiesen saber en cuales bases de datos se encuentra su información, pudiendo acceder al registro. De esa forma, sería más simple realizar un seguimiento de los datos y probar que efectivamente existieron cesiones a terceros. Así, el titular sabría por qué le están realizando marketing directo a su teléfono celular, sin que haya consentido en algún momento en darle su información a determinada empresa.

De igual forma, el que no exista hoy en día una autoridad de control de datos personales en nuestro país, conlleva entre uno de sus problemas el reporte efectivo de brechas de datos. Este aspecto lo trataremos con mayor amplitud en el capítulo dedicado a la seguridad de datos, pero es importante destacar que, al no existir un deber de reportar brechas de seguridad, ni una autoridad de control al respecto, el titular no tiene cómo saber cuándo se produjo la filtración de su información que desencadenó un daño, viéndose imposibilitado, por ejemplo, a tomar las precauciones del caso para mitigar posibles daños. Un ejemplo clásico de esto puede ser la filtración de datos de tarjetas bancarias o de datos

de salud. Al no existir una autoridad de control ni una obligación de reporte a dicho organismo, los titulares pueden saber días o semanas después que su información personal se vio expuesta[88].

En lo que respecta al régimen general de indemnización, estamos de acuerdo en que se necesita un reforzamiento del actual y el establecimiento de reglas claras y especiales para ello. A nuestro parecer es incorrecta la denominación de "sistema sectorial" que realiza Corral[89], respecto del tratamiento de datos, ya que, en lo medular del sistema indemnizatorio, este se remite a las reglas generales.

Parada igualmente comparte la urgencia de un cambio en este aspecto, proponiendo la exigencia de una responsabilidad con inversión de la carga de la prueba que actualmente soporta el titular, dejándola ahora en manos del responsable[90].

Acá hay que realizar una precisión y es que, por aplicación de las reglas generales, lo que desprendemos es que ya existe inversión de la carga de la prueba, debido a que el legislador realiza exigencias de "debida diligencia" dentro de la LPD, siento el ejemplo específico el caso del artículo 11°. En ese sentido, a nuestro juicio la idea detrás de la propuesta anterior sería que existiera una inversión de carga de la prueba en todos los casos en que se accione por responsabilidad civil en virtud de la LPD y no únicamente en los casos en que lo que exista sea una aplicación de reglas generales, en tanto que la prueba de la diligencia recae en quien debió emplearla. Volveremos ampliamente a esto en el próximo capítulo al hablar específicamente de este artículo de la LPD.

A su vez, también identificamos un problema en que no exista una regla similar a la que existe en el GDPR respecto al tratamiento en que intervengan muchos responsables y/o encargados. En ese sentido, en nuestra legislación no se establece el supuesto de responsabilidad solidaria que sí consagra la normativa europea, con lo cual no existe esta facilidad de exigir una indemnización por parte del titular a la hora de verse enfrentado a verdaderas redes de tratamiento y transferencia de datos, que pueden implicar el empleo de una serie de tecnologías y/o procedimientos que, a final de cuentas, tendrían la capacidad

[88] Esto es particularmente problemático en el sentido de generar los incentivos suficientes para que el responsable informe a la autoridad de control de una brecha de datos. Una forma sería establecer un sistema de multas muy duro, como es el caso del GDPR, ya que, si no se establecen multas ejemplificadoras, perfectamente los responsables podrían omitir el reporte o posponerlo para mucho tiempo después, ya que su imagen corporativa podría verse mermada.
[89] CORRAL, H. 2004. Lecciones de Responsabilidad Civil Extracontractual. Santiago, Editorial Jurídica de Chile. 271-273pp.
[90] PARADA, B. *op. cit.*, 84-85pp.

de terminar dificultando tanto la persecución de la responsabilidad civil, como el ejercicio de otros derechos del titular.

Ahora que ya fueron revisadas las principales virtudes y falencias del régimen de responsabilidad civil general de la LPD, pasaremos a estudiar una indemnización específica, que es la correspondiente a la infracción al deber de seguridad de los datos personales.

CAPÍTULO III: El PRINCIPIO DE SEGURIDAD DE DATOS PERSONALES Y SU EXISTENCIA EN LA LEGISLACIÓN CHILENA

En el presente capítulo, luego de haber abordado de forma general el marco regulatorio de la protección de datos personales en Chile y su régimen de responsabilidad civil, analizaremos el principio de seguridad de datos personales, presentando en forma general el artículo 11° de la LPD en el que se ha entendido se encuentra incorporado éste y verificar su presencia efectiva. Esto nos permitirá luego analizar, en el próximo capítulo, las implicancias que hoy en día esta disposición en el ejercicio de la acción de indemnización de perjuicios.

Para complementar el análisis, también revisaremos en este capítulo el tratamiento comparado que se le da al deber de seguridad de datos personales, a la vez que pondremos especial atención en lo que se entiende por "medida de seguridad", para así comprender en qué consiste la manifestación concreta de este deber.

1. EL PRINCIPIO DE SEGURIDAD DE DATOS EN NUESTRA LEGISLACIÓN

Tal como fue esbozado en el primer capítulo de este trabajo, la protección de datos ya sea desde un punto de vista de derecho interno o comparado, tiene una serie de principios que informan toda la legislación y funcionan como base sobre la que se erige el entramado normativo al respecto. Tal como indica Arrieta "*éstos son una serie de preceptos informadores, con pretensión de carácter universal, que han de inspirar la forma y la oportunidad en que se desarrolla el tratamiento de datos personales por parte de los responsables del mismo y de los bancos de datos*"[91].

Uno de estos principios es el principio de seguridad de datos personales, que se encuentra en el artículo 11° de la LPD, el cual indica lo siguiente:

> "*Artículo 11.- El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños*".

[91] ARRIERTA, R., *op. cit.,* 16p.

Como primer punto a tratar en este capítulo, analizaremos qué se entiende por el principio de seguridad de datos y nos referiremos respecto de si se encuentra efectivamente incorporado a nuestra legislación en virtud de la disposición precedentemente citada.

- El principio de seguridad de datos

Tal como adelantamos en el primer capítulo, el principio de seguridad implica una protección de la información en sí, siendo una de las ideas basales sobre las que se fundamentan las distintas normativas de protección de datos y que en virtud de este principio lo que pretenden es la protección o cuidado de la información personal de posibles injerencias que puedan afectarle.

Es de común entendimiento que en nuestra sociedad actual el dato se ha convertido en insumo fundamental de cualquier proceso económico, existiendo un exponencial desarrollo, en los últimos años, de las técnicas y destrezas para su tratamiento que han generado que cada vez sea mayor el valor que se pueda extraer de la información personal y, "*que han hecho posible que en torno al dato se generen modelos de negocio hasta hace poco inimaginables, por inviables*"[92]. Pues bien, esta información de creciente valor desde hace ya décadas que se ha entendido necesaria de proteger, no solo por su aspecto económico, sino también por la importancia que tiene para los titulares de los datos respecto a la protección de sus derechos fundamentales. Es en este orden de ideas que se erige el principio de seguridad de datos, el cual implica la exigencia de que el responsable cuide los datos que están en su poder, entendiendo la necesidad de que "*se adopten medidas apropiadas para proteger los bancos de datos contra riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informático*"[93].

Las diferentes leyes de protección de datos reconocen este principio buscando que, junto con brindar garantías jurídicas para el efectivo resguardo de los derechos de los titulares frente a los riesgos que presenta el tratamiento de datos, también se le otorga un especial énfasis al cuidado que se le debe dar a los datos, manifestando deberes de adopción de medidas de seguridad relativas a cautelar esta información. En este sentido la seguridad de datos implica que "*el tratamiento de datos personales supone la realización*

[92] FUNDACIÓN TELEFÓNICA. 2017. Economía de los Datos: Riqueza 4.0. Madrid, Editorial Ariel S.A. 7p.
[93] JERVIS, P. 2006. La regulación del mercado de datos personales en Chile. *op. cit.*, 65p.

de un conjunto de operaciones, manuales o automatizadas, las que para evitar perder el control de la información requieren implementar medidas tecnológicas y de procesos orientadas a asegurar los datos y detectar oportunamente cualquier acceso no autorizado a los mismos"[94].

A mayor abundamiento, Garrido plantea al principio de seguridad de datos como un deber impuesto sobre el responsable, indicando que "*seguridad se define como la serie de medidas técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, cualquiera sea el método de tratamiento, particularmente a través de las redes de comunicación. Estas medidas deben aplicarse en niveles o en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse*"[95].

Así, sintetizando, la seguridad de datos es un principio rector de la legislación de protección de datos y que supone una exigencia para el responsable de cuidar los datos frente a las posibles injerencias que éstos puedan sufrir, debiendo adoptar medidas se seguridad que tiendan a asegurar esta protección. En ese sentido, este deber gira en torno, precisamente, a la adopción de estas medidas de seguridad de datos personales, ya sea desde el punto de vista de su efectivo establecimiento o no, así como de las afectaciones que los datos puedan recibir por el quebrantamiento de estas medidas tomadas o por no haber existido al momento de la injerencia.

Antes de proseguir con el análisis, creemos que también es necesario realizar una diferenciación clara de lo que se entiende por seguridad de datos de otros principios que, a una primera lectura, podrían sonar indistinguibles. En específico, pueden aparecer particularmente indistintos el deber de seguridad y el deber de secreto, y esta no es una cuestión que pueda ser entendida como un grave error si no se está adentrado en la materia, ya que al estar fundamentada en la privacidad la protección de datos, una forma de entender la seguridad ante este bien jurídico sería, precisamente, el secreto de la información.

---

[94] ARRIETA, R. 2011. Autorregulación y protección de datos personales. En: Reflexiones sobre el uso y abuso de los datos personales en Chile. Santiago, Expansiva. 20p. [en línea] <https://www.consejotransparencia.cl/category_estudios/publicaciones-cplt/> [consulta: 23 de diciembre de 2018]

[95] GARRIDO, R. 2015. La seguridad en el tratamiento de datos personales. En: Ciudadanas 2020 III: El gobierno de la información. Instituto Chileno de Derecho y Tecnología. 82-83pp.

Para despejar esta duda, tenemos que entender que el deber de secreto se encuentra en el artículo 7°[96] de la LPD y que, en términos sucintos, consiste en que *quienes trabajan en el tratamiento de datos personales están obligados a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos*[97]. Por su parte, el deber de seguridad, si bien también opera como un deber a cumplir por el responsable, su énfasis se encuentra en las medidas a tomar para una protección de los datos frente a agentes externos, siendo una práctica común el que el legislador le imponga la adopción de medidas de seguridad de diversas índoles[98] (físicas, lógicas, etc.), con tal de resguardarles.

En este sentido, el "secreto de los datos" es una imposición de confidencialidad que recae sobre el responsable, sus dependientes, y todo aquel que trabaje respecto del tratamiento de datos; por su parte, la "seguridad de los datos" hace referencia a las medidas de protección y al celo con los que el responsable cuida los datos que están bajo su poder. A continuación, será planteado un ejemplo práctico para diferenciarlos de mejor manera.

Imaginemos el caso del trabajador de una clínica que tiene acceso a los distintos diagnósticos y exámenes médicos de los pacientes. Estos documentos contienen una serie de datos personales, como los nombres, domicilios, números de RUT, y por, sobre todo, datos de salud de los pacientes, y son manejados de diversas formas y para variados fines en este recinto asistencial. Si alguno de los profesionales que trabajó en la toma de exámenes o en la elaboración de informes o cualquier otro asociado a la información de salud, divulgase en sus redes sociales que determinado paciente padece cáncer o VIH, allí se estaría infringiendo el deber de secreto. Esto se debe a que se está divulgando la información personal a la que se tuvo acceso debido a las funciones que se ejercían en el contexto del tratamiento de datos, y que no fueron obtenidos de fuentes accesibles al público. Acá, la confidencialidad se destruyó desde dentro, desde un agente que se encontraba en el contexto del tratamiento y no desde fuera.

[96] Artículo 7°. Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo.
[97] CERDA, A., *op. cit.,* 26p.
[98] *Loc. cit.*

En el mismo caso, pero en esta ocasión ocurriese una filtración de la información personal debido a que los servidores de la clínica no contaban con medidas técnicas de seguridad, siendo fácilmente hackeados. Acá se está infringiendo el deber de seguridad por cuanto se está permitiendo el acceso a los datos que, se suponía, debían de estar seguros en manos del responsable.

Para la infracción del deber de secreto es necesario que sea una persona que tuvo acceso a los datos, debido al ejercicio de sus funciones, la que divulgue la información. Por su parte, la infracción al deber de seguridad no necesariamente supone una divulgación pública o privada, ya que se quebrantaría este deber en el momento en que la información fue accesible por terceros que no están autorizados para ello, no siendo necesario que se ponga a disposición del público ni que sea comunicada. En ese sentido, lo importante a la hora de hablar de seguridad, es que los datos se queden íntegramente con quién es el responsable y con nadie más, ya que es él quien se encuentra facultado para su tratamiento y quien debe propender a que la información no sea accesible, bajo ningún concepto, por personas que no tienen legitimidad, debiendo adoptar las debidas medidas de seguridad para su protección. Dicho en otros términos, en este deber se pretende evitar la sustracción o acceso de terceros a los datos, siendo principalmente el hackeo de bases de datos la práctica que comúnmente se encuentra en conflicto con este principio del tratamiento. En este sentido, Jervis nos indica que "*la confidencialidad* [deber de secreto] *se refiere al mayor o menor secreto en que se van a guardar y tratar esos datos; y, la seguridad* [deber de seguridad] *hace referencia a las medidas de protección a tomar para la mejor defensa de la privacidad y grado de confidencialidad*"[99], pero a la vez destaca que el legislador no ha considerado la concretización de este principio que supone la adopción de las medidas de seguridad de datos.

A mayor abundamiento, como señala Osvaldo Gozaíni[100], en este principio se precisa un cierto grado de seguridad técnica que impida que la información se corrompa, destruya, o inutilice por casos fortuitos o "riesgos naturales", asimismo, se necesita seguridad lógica que impida que terceros no autorizados accedan a la información personal, que les permita por ejemplo, efectuar usos, modificaciones o divulgaciones indebidas de la misma. Lo anterior es muy importante para aportar a la diferenciación del principio de seguridad de otros principios del tratamiento, en tanto que apunta a las medidas de carácter técnico para

[99] JERVIS, P., *op. cit.*, 66p.
[100] Gozaini, Osvaldo. 20010. Hábeas data. Protección de datos personales. Doctrina y jurisprudencia. Buenos Aires. Rubinzal-Culzoni. p. 204. Citado en: JERVIS, P., *op. cit.*, 65p.

resguardar íntegramente la información personal; así como una dimensión de seguridad logística por parte del responsable de datos, la cual permita hacer frente al acceso sin autorización que se podría tener de esta información.

- La seguridad de datos en el artículo 11° LPD

Una vez despejado lo que implica el principio de seguridad de datos, pasaremos a revisar la disposición en que se ha entendido que se encuentra incorporado en nuestra legislación y que es el artículo 11° de la LPD que en las primeras páginas de este capítulo citamos.

Nuestra doctrina ha entendido que precisamente es en este artículo en el que se manifiesta el principio de seguridad de datos personales, al establecer una exigencia de debido cuidado por parte del responsable del registro o banco de datos una vez captada la información personal. Correlativa a esta exigencia, el legislador dispone que el responsable debe indemnizar los perjuicios derivados de la inobservancia de esta norma.

En este sentido, al referirse al principio de seguridad de datos, Cerda indica que "*si bien nuestro legislador impone al responsable del registro o banco de datos el deber de cuidar de ellos con la debida diligencia, haciéndole inclusive responsable de los daños, no ha prestado atención alguna en cuanto a las medidas concretas que han de aplicarse para brindar un adecuado nivel de cuidado de los datos*"[101].

De igual manera, Violler ha dicho que el principio de seguridad de datos "s*e encuentra recogido en el artículo 11 de la Ley 19.628, que establece la obligación del responsable de los registros o bases donde se almacenen datos personales, de cuidar de ellos con la debida diligencia, haciéndose responsable de los daños causados*"[102]. Del mismo tenor, Rajevic apunta expresamente a que el principio de seguridad se encuentra contemplado y cautelado en el artículo 11° de la LPD[103].

En esta línea y tal como mencionamos anteriormente, Jervis también alude a que el artículo 11° de nuestra LPD se identificaría con el principio se seguridad, mencionando

[101] CERDA, A., *loc. cit.*
[102] VIOLLIER, P. 2017. El estado de la protección de datos personales en Chile. Santiago, ONG Derechos Digitales. 23p. [en línea] <https://www.derechosdigitales.org/tipo_publicacion/publicaciones/> [consulta: 12 enero 2019]
[103] Rajevic, Enrique. 2011. Protección de datos y transparencia en la administración pública chilena: Inevitable y deseable ponderación. En: Reflexiones sobre el uso y abuso de los datos personales en Chile. Santiago, Expansiva. 144p. Disponible en línea: <https://www.consejotransparencia.cl/category_estudios/publicaciones-cplt/> [consulta: 23 de diciembre de 2018]

que este artículo obliga al responsable de datos (sea público o privado) a indemnizar el daño que causare por el tratamiento cuando no se hubieren adoptado todos los resguardos técnicos necesarios para evitar un error en el almacenamiento de ellos[104].

Por su parte el Comité de Evaluación de la Ley de la Cámara de Diputados en informe relativo a la LPD, cuando trata el principio de seguridad manifiesta que este principio impone al responsable el deber de adoptar todas las medidas que sean necesarias para el tratamiento de datos, aludiendo a que en el artículo 11° de esta ley se contempla este deber de cuidado que recae sobre el responsable, pero que, sin embargo, no contempla en forma clara las medidas de seguridad de datos que serían la concreción de este principio y la vara a utilizar para verificar si es que el responsable cumple con la norma[105].

Finalmente, también podemos mencionar lo planteado por Garrido[106] al referirse a este tema, quien precisa que, a diferencia de los instrumentos internacionales, la LPD no señala expresamente la seguridad de datos, sino que indica en el artículo 11° el deber del responsable de efectuar el tratamiento con un cuidado diligente, lo cual a su parecer es un concepto bastante amplio y que variaría caso a caso.

Sintetizando, las posturas doctrinarias y de los legisladores respecto a este tema es que el principio de seguridad de datos se encuentra en el artículo 11°, con salvedad de que no se especifican, de forma expresa, las medidas de seguridad que se deben adoptar en virtud de este principio. Esto último es de común opinión respecto de este principio en nuestra legislación y que se identifica como una de las principales falencias de nuestra actual LPD a la hora de referirse a la seguridad de datos, en comparación al tratamiento comparado en la materia, el cual veremos más adelante.

Para un análisis más acabado, comentaremos la principal jurisprudencia en materia del artículo 11° de la LPD, la cual identificaremos como "El Caso de Santander" y que caracterizaremos brevemente.

- El Caso Santander

[104] JERVIS, P., *op. cit.*, 154p.
[105] COMITÉ EVALUACIÓN DE LA LEY/OCDE. 2016. Evaluación de la Ley N° 19.628. 32p. [en línea] <http://www.evaluaciondelaley.cl/informes-leyes-evaluadas/foro_ciudadano/2012-12-11/164002.html> [consulta: 25 de diciembre de 2018]
[106] GARRIDO, R., *op. cit.*, 79-80pp.

Durante los primeros días de octubre del año 2015, diversas personas fueron contactadas por vía telefónica por un periodista de TVN, quien les informó que se había encontrado importante documentación de carácter personal referida a cada uno de ellos abandonada en la ruta G-68, a un costado de la Cuesta Barriga. Entre estos documentos había copias de cédulas de identidad, estados de situación financieros, liquidaciones de sueldo, etc. Ante la llamada, muchas personas a las que les concernía la información concurrieron al lugar, donde pudieron constatar la efectividad de lo dicho por el periodista, encontrando un gran número de carpetas y documentos con información entregada o generada por el Banco Santander Chile. Era tal la cantidad de datos personales que contenían los documentos dejados en el basural, que con la sola información que allí se encontró, fue posible para el equipo de TVN el contactarlos. Finalmente, cabe destacar que estos desechos no fueron dejados por personal directo de Santander, sino que por una personal de una empresa contratada por el banco.

Ante esta situación, varias de estas personas dedujeron acciones de indemnización de perjuicios por vulneraciones a la LPD, entre las que se encuentra la seguridad de datos del artículo 11°[107].

En el caso Ampuero con Banco Santander, el tribunal de primera instancia en su considerando undécimo sentenció que la LPD obliga al responsable a observar una debida diligencia respecto a los datos que recopila, **desde su almacenamiento hasta su destrucción o cancelación, incluyendo todo tratamiento de datos que ocurra en el intertanto**.

A la vez, prosigue aludiendo a que esta institución bancaria, en el curso de las actividades de su giro mantiene información personal de sus clientes o solicitantes, contando con un vasto banco de datos sobre una multitud de personas. Como responsable de un banco de datos, se encuentra dentro del ámbito de aplicación de la LPD. De ello, se sigue que tiene el deber institucional de dar pleno cumplimiento al artículo 11° de esta ley, por lo que aun cuando en el caso la información personal haya terminado en un vertedero por error de un dependiente, correspondía al responsable de datos la obligación de tener el

[107] En efecto, existen varias causas en base a estos mismos hechos y cuyo tenor de discusión fue prácticamente idéntico. En este trabajo no pretendemos hacer un análisis pormenorizado de cada una, sino que tomar las principales consideraciones de la jurisprudencia en uno de estos casos y verificar que se aplicó el artículo 11° LPD en cuanto a la seguridad de datos. En este sentido, podemos mencionar las causas: ARELLANO / BANCO SANTANDER (5 J.L. Santiago rol N°C-29211-2015 y Corte de Apelaciones de Santiago rol N°11788-2017); y AMPUERO/ BANCO SANTANDER (16 J.L. Santiago rol N°C-29221-2015, firme y ejecutoriada).

cuidado suficiente con los datos personales de sus clientes, de tal forma que fuese imposible que se produjese la confusión que se alegó en la causa.

En el mismo considerando anteriormente citado, el tribunal agregó que la cadena de actos que culminó con los documentos que contenían información privada de los demandantes se inicia por el descuido del banco, esto es, habría sido imposible que acabaran en un basural clandestino en la Cuesta Barriga si Banco Santander Chile hubiese tratado los papeles en cuestión con la diligencia esperable de una institución importante que trabaja con datos personales. El dejar cajas llenas de papeles íntegros con información privada junto con escombros y basura de una remodelación, a juicio del tribunal, está lejos de aquello que la experiencia de un hombre medio dicta como adecuado o correcto.

En virtud esto y otras consideraciones, el tribunal en este caso sentenció a una indemnización de dos millones de pesos por concepto de daño moral. Esta sentencia no fue recurrida ante la Corte de Apelaciones respectiva y se encuentra actualmente firme y ejecutoriada.

Este caso es muy útil para el análisis de la seguridad de datos en nuestro país, ya que nos facilita desprender que sería efectiva la exigencia de seguridad de datos que pesa sobre el responsable en virtud del artículo 11° de la LPD, lo que se condice con lo planteado por la doctrina citada, con independencia de que nuestro legislador especifique o no las medidas de seguridad concretas a adoptar. A la vez, nos permite perfilar que en sede jurisdiccional se ha delimitado la extensión de esta exigencia de seguridad, indicándose que, hasta su destrucción o cancelación, incluye todo tratamiento que suceda en el intertanto.

Ahora bien, a nuestro parecer este caso tuvo, en general, un final favorable para los demandantes, gracias a que fue una situación mediática y cubierta por los medios, lo que aportó mucho a la hora de presentar prueba en favor de acreditar que fueron dejados estos documentos en el vertedero y que ello era atribuible al actuar negligente de Santander. De igual forma, cabe destacar que las pruebas ofrecidas por las partes a este respecto aportaron a facilitar la determinación de la manifiesta falta de diligencia, por lo que la facilidad del establecimiento de la responsabilidad civil en el caso es más bien muy excepcional.

Por contrario, en un caso en que no hubiese existido tal cosa como una investigación periodística, sería todavía más difícil demostrar o conocer los hechos y obtener una indemnización. Por ejemplo, una brecha de seguridad informática se da en el contexto

interno de una empresa o servicio público, siendo un hecho claro que el titular no necesariamente va a saber cómo ni dónde ocurrió, ni tampoco si es que la brecha es atribuible a negligencia del responsable. Esto último en el caso en análisis era más bien de fácil consideración, sobre todo ya que es por una cuestión de lógica natural, el que a todas luces sea negligente dejar información personal a disposición de cualquier persona en un vertedero clandestino.

2. LA SEGURIDAD DE DATOS EN EL ÁMBITO COMPARADO

Una vez planteado de forma general el principio de seguridad de datos personales y su consagración en el artículo 11° de nuestra LPD, es necesario analizar el tratamiento comparado que se le ha dado, para posteriormente revisar qué son las medidas de seguridad. En este sentido, la finalidad principal que tendrá, para efectos de este trabajo, realizar un estudio comparado del tratamiento de la seguridad de datos, se debe a que las infracciones a este deber suponen infracciones a la normativa de protección de datos y, tal como indicamos en el capítulo anterior, las infracciones a las distintas leyes de protección de datos que irroguen daños al titular pueden dar lugar a indemnización de perjuicios a su favor. Es decir, el quebrantamiento de la seguridad de los datos personales **puede significar el ejercicio de una acción de indemnización de perjuicios**, cuando éstos se deriven de ello.

Las normativas comparadas a analizar son las siguientes:

a. GDPR

Tal como ya hemos indicado a lo largo de este trabajo, el GDPR es hoy en día la normativa cabecilla a nivel mundial en lo que a tratamiento de datos se refiere. En este sentido, el principio de seguridad de datos es tratado de forma íntegra y orgánica a lo largo de esta normativa, siendo uno de los aspectos que más considerandos y artículos toma.

De esta forma, su considerando[108] 49° indica que la seguridad es un interés legítimo del titular de datos (que en esta normativa se denomina "interesado"). De igual forma, en el considerando 83° manifiesta que a fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el reglamento, el responsable debe evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlo, debiendo con ellas garantizar un nivel de

[108] Las normativas de la Unión Europa, consistente tanto en considerandos ("*recitals*" en inglés), como en artículos. Ambos son muy importantes, por cuanto, si bien los segundos consisten en la norma positiva, los primeros suponen las motivaciones, fundamentos y directrices que se tuvieron a la vista para la elaboración de la norma, teniendo un gran valor interpretativo.

seguridad adecuado, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. En conjunción con ello, a nuestro parecer el considerando más importante en esta materia es el 85°, por cuanto destaca que, si no se toman a tiempo medidas de seguridad adecuadas, las violaciones de seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas. Acá se hace presente la vitalidad de las medidas de seguridad para esta normativa, por cuanto su no o incorrecta adopción, puede desembocar en serios riesgos para los intereses del titular de datos.

Por su parte, en su artículo de definiciones, se indica que una violación de la seguridad de los datos personales significa: "*toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*"[109]. Acá lo que se realiza es una delimitación de qué supone el quebrantamiento de las medidas de seguridad de datos, lo que nos perite entender de qué habla la regulación cuando se refiere a una infracción a la seguridad, es decir, de no adoptarse las debidas medidas de seguridad apropiadas, lo que puede ocurrir es una violación de la seguridad de los datos y, de ocurrir, se estaría infringiendo con la normativa. Esto se relaciona con lo dispuesto en el artículo referente a **los principios del tratamiento de datos**[110], en el cual se indica que los datos deberán ser tratados de tal manera que **se garantice una seguridad adecuada** de ellos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Una vez planteados estos artículos de carácter más general, el GDPR en su artículo 32° y siguientes trata, específicamente, la seguridad del tratamiento. Indica que teniendo en consideración el estado de la técnica, los costes y su naturaleza, así como los contextos y fines del tratamiento, se deberán adoptar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento. Por su parte, uno de los elementos más importantes al regular la seguridad del tratamiento, es qué se realiza si es que son vulneradas las medidas de seguridad (o las consecuencias que pudiesen ocurrir por su no adopción). En ese sentido, dispone que, en caso de violación de la seguridad de los datos personales, el responsable del tratamiento notificará a la autoridad

[109] GDPR, artículo 4° N° 12
[110] GDPR, artículo 5° letra f.

de control competente a más tardar dentro de 72 horas. A la vez, cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades del titular, el responsable del tratamiento le comunicará sin dilación indebida.

La finalidad de esta revisión particular del GDPR ha sido precisar de qué forma la normativa más importante de tratamiento de datos, regula el principio de seguridad y la adopción de las medidas para cumplir y asegurar la debida seguridad de los datos personales. En este sentido, es muy importante destacar no solo, que siempre se relaciona seguridad de datos con adopción de medidas de seguridad, suponiendo la una a la otra, sino que, también, es recalcable la relación que se tiene con el regulador, por cuanto permite la coordinación para la respuesta a las brechas de seguridad, así como la mitigación de los posibles daños que se puedan provocar como derivados de ellas, lo cual puede ser de gravitante importancia en sede de indemnización de perjuicios.

b. Estados Unidos

En lo que respecta al tratamiento que se le da en Estados Unidos, tenemos que volver a destacar, tal como indicamos en el primer capítulo, que la regulación de la protección de datos se encuentra dispersada de forma sectorial, dependiendo de la industria, actividad, así como entre Estados[111].

En ese sentido, podemos la Health Insurance Portability and Accountability Act ("HIPAA"); y la Financial Services Modernization Act (denominada como "Gramm-Leach-Bliley Act"). Ambas tratan entre sus disposiciones la seguridad de la información personal, cada uno en su rubro particular y adecuado a su materia; la primera en materias de salud; la segunda en materias relativas al sector financiero.

Con todo, quisiéramos destacar el tema de las brechas de seguridad de información personal y su tratamiento normativo en Estados Unidos. A este respecto, California fue el primer Estado en promulgar en su legislación una obligación de notificación de brechas de seguridad de información (California Civil Code §1798.82), en el que se consagra en favor de todos sus habitantes que serán notificados de las brechas de seguridad de datos personales que les conciernan, debiendo ésta tener determinadas menciones y

[111] Para más información, recomendamos ver el análisis ofrecido en: IEUAN, J. 2018. Data protection in the United States: overview. [en línea] <https://uk.practicallaw.thomsonreuters.com/6-502-0467> [consulta: 24 de diciembre de 2018]

formalidades, entre las que se encuentra la individualización de lo ocurrido, la determinación de la fecha de la brecha y cuál fue información que se vio envuelta.

Esto es puntualmente valorable por cuanto, tal como indicamos anteriormente, la efectiva y pronta notificación para el regulador y el titular, suponen una respuesta más efectiva ante brechas de seguridad de datos y, con ello, es posible mitigar los posibles daños que pudiesen ocurrir por la filtración de la información personal.

c. México

Tal como hicimos referencia en el capítulo anterior, la legislación mexicana es de las más desarrolladas en el ámbito latinoamericano y, como es de esperar, también trata la seguridad de los datos personales. En específico, en el artículo 19° y siguientes de su ley de protección de datos se indica que todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. A la vez, se establece que los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo, se deberá tomar en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

Por su parte se prescribe[112] que las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.

Finalmente, se indica explícitamente[113] que constituyen infracciones a la ley la vulneración a la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable.

A nuestro parecer es muy destacable lo que realiza la legislación mexicana a este respecto por cuanto precisa de forma muy completa (similar al tratamiento que le da el GDPR) lo que implica la seguridad de los datos. En este sentido, indica qué se debe realizar en virtud de este deber, así como indicar expresamente la necesidad de notificar

[112] LFPDPPP, artículo 20°
[113] LFPDPPP, artículo 63° N° XI

una brecha de seguridad en los casos en que se puedan ver afectados los derechos patrimoniales y morales de los titulares. Esto último es especialmente valorable, ya que se desprende que la o una de las finalidades de esta información es que el titular pueda tomar las medidas correspondientes para proteger sus derechos.

d. Argentina

Para un estudio más acabo, es útil revisar lo que ocurre en Argentina para visualizar cómo se tratan estas materias en el ámbito sudamericano. En el país trasandino también existe tratamiento del deber de seguridad de datos, pero no de manera muy desarrollada. En este sentido, en el artículo 9° de su ley de protección de datos se indica que el responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar afectaciones[114] y que permitan detectar desviaciones de información. A su vez, se prohíbe registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

A nuestro parecer es insuficiente únicamente indicar de forma general en qué consiste la seguridad de datos, sin darle un aterrizaje concreto, así como resulta problemático no establecer obligaciones de notificación de brechas de seguridad de datos. Con todo, y tal como se ha esbozado anteriormente es, en principio, más específico de lo que actualmente ocurre en la legislación de nuestro país respecto de la seguridad de datos.

Sintetizando este apartado, tal como podemos ver la seguridad de datos tiene como denominador común el establecimiento por parte del legislador de una obligación de adopción de medidas de seguridad que propendan a garantizar un tratamiento seguro, que protege el contenido de la información personal.

3. LAS MEDIDAS DE SEGURIDAD DE DATOS

Ahora que ya revisamos en general el tratamiento nacional y comparado de la seguridad de datos personales, es muy importante detenernos en el aspecto específico al que las normativas se refieren cuando hablan de seguridad de datos, y que son las denominadas “medidas de seguridad”.

Las medidas de seguridad son la manifestación concreta del principio de seguridad de datos personales y, tal como su nombre lo indica, suponen una serie de disposiciones que

[114] Acá se plantean como ejemplos la adulteración, pérdida, consulta o tratamiento no autorizado.

el responsable de datos adopta para resguardar los datos personales contra posibles injerencias que puedan afectarles, como su destrucción, pérdida, alteración, acceso no autorizado, entre otras.

Se ha distinguido[115] que las medidas de seguridad pueden diferenciarse en medidas técnicas y en medidas organizativas. Las primeras hacen referencia al conjunto de controles de carácter tecnológico que implementa un responsable y que le permiten hacer frente a los riesgos a los que está sujeta la información personal[116], como por ejemplo software destinado a la protección de bases de datos; por su parte, las segundas corresponden al conjunto de medidas de seguridad incluidas en los procesos y estructuras existentes en la organización y que tienen por finalidad principal manejar la complejidad de los procesos de gestión de la seguridad y dar respuesta a los riesgos, condicionantes normativos y regulatorios[117], como pueden ser los protocolos de seguridad informática internos de una empresa. A su vez, ambos tipos de medidas deben aplicarse en relación con los riesgos específicos que presente el tratamiento del que se trata y/o con la naturaleza de los datos que deban protegerse.

Respecto de las medidas de seguridad, Garrido identifica[118] una serie de elementos que les caracterizarían:

i. Las medidas de seguridad se aplican con independencia de si el tratamiento es informatizado o manual.

ii. Deben distinguirse la finalidad, uso y naturaleza de los datos para su aplicación según niveles o riesgos[119].

iii. Las medidas pueden segregarse, pero solo si es posible eliminar datos. Si no es posible esta operación, se debiesen de aplicar siempre las medidas con un nivel más alto o aquellas aplicables a los datos que presenten un mayor riesgo.

[115] GARRIDO, R., *op. cit.,* 83p.
[116] GARRIDO, R., *op. cit.,* 87p.
[117] GARRIDO, R., *op. cit.,* 84p.
[118] GARRIDO, R., *op. cit.,* 83p. Cabe destacar que estos elementos comunes se desprenderían del tratamiento comparado más desarrollado que se les da, ya que las posibles exigencias respecto a las medidas de seguridad que caracteriza, así como la diferenciación en tipos, no se encuentran en nuestra LPD.
[119] En derecho comprado, por ejemplo, en legislación europea como la española, se diferencian niveles de seguridad, los cuales suponen que ciertas medidas son de un carácter básico a la hora de proteger datos, mientras que otras tienen nivel mayor y cuya adopción dependerá del tipo de datos que son tratados.

iv. Deben tener un control permanente, periódico y constante.

v. Son aplicables sobre bases de datos temporales o permanentes, en tanto que se atiendo al contenido del dato personal que se protegerá.

vi. Se concretizan en un documento de seguridad elaborado por el responsable de datos, que deberá ser acorde a la normativa vigente, mantenerse actualizado y ser obligatorio para todo el personal de su organización.

En este entendido, con la adopción de medidas de seguridad, tanto técnicas como organizativas de nivel adecuado, se lograría cumplir con el objetivo de garantizar el cuidado de los datos, lo que implica su disponibilidad, integridad y confidencialidad. Específicamente estos aspectos implican[120]:

- Disponibilidad: Conlleva asegurar que únicamente los usuarios autorizados tengan acceso oportuno a los datos personales, en los momentos en que se requieran.
- Integridad: Que los datos los que se acceda se mantengan íntegros, exactos, correctos y completos.
- Confidencialidad: Los datos deben ser conocidos y accedidos solo por quienes están autorizados, lo que implica que su contenido sea reservado.

Así, en resumidas cuentas, el objetivo de las medidas a adoptar para asegurar los datos personales conlleva que éstos no sean alterados (integridad); que se encuentren siempre disponible, evitando su pérdida y teniendo el completo control sobre su acceso (disponibilidad); y evitarán que se logre tener acceso a ellos por parte de personas sin la autorización correspondiente (confidencialidad).

Tenemos que tener en consideración que la adopción de medidas de seguridad es importantísima desde un punto de vista regulatorio, por cuanto la entidad de control las verifica y las evalúa para poder determinar la multa aplicable en casos de infracciones a este deber que pesa sobre el responsable. En este sentido, en Europa, una de las razones para el gran plazo que existió entre la aprobación y entrada en vigencia del GDPR (adoptado en 2016 y entrado en vigencia el 2018) fue que las empresas pudieran adaptarse a las medidas que debían adoptar para cumplir con los requerimientos de la normativa,

[120] GARRIDO, R., *op. cit.*, 83-84pp.

entre las que se encontraban la seguridad de datos, desde un punto de vista de medidas de seguridad, así como de organización interna y relación con el regulador. Así, hoy en día uno de los elementos más importantes para la elaboración de una línea de costos en un determinado negocio (y que además conlleva un gran gasto en servicios de asesoría jurídica al respecto) es el *compliance* relativo a las disposiciones de seguridad de datos que se deben cumplir conforme al GDPR.

CAPÍTULO IV: ANÁLISIS CRÍTICO DE LA SEGURIDAD DE DATOS EN NUESTRO PAÍS

Una vez visto el tratamiento nacional y comparado que recibe el principio de seguridad de datos y habiendo realizado una revisión de su manifestación concreta que son las medidas de seguridad, en este capítulo pasaremos a analizar la responsabilidad civil derivada de infracciones al artículo 11° de la LPD y si es que supone un problema para el titular de datos que su actual redacción no especifique las medidas de seguridad de datos que debiese de adoptar el responsable en virtud de este principio.

1. EL ARTÍCULO 11° LPD Y RESPONSABILIDAD CIVIL

Como planteamiento previo, es necesario indicar el régimen de responsabilidad civil en este caso. Tal como trabajamos en el capítulo anterior, el régimen de responsabilidad civil por infracciones a las disposiciones de la LPD se encuentra en su artículo 23°. En ese sentido, es importante identificar la diferencia en la tramitación que presentan las infracciones cuando se deniega el ejercicio de derechos del titular, ya que la acción de *habeas data* supone un procedimiento regulado en otras disposiciones de este cuerpo normativo, mientras que, el resto de las infracciones se subsumirían en lo dispuesto en el artículo en comento.

De esta forma, las infracciones al artículo 11° de la LPD suponen la tramitación de un juicio sumario ante el juez de letras de domicilio del responsable, tal como se desprende el artículo 23° del mismo cuerpo normativo. A su vez todas las generalidades del régimen de responsabilidad civil de la LPD se siguen en estos casos, no presentando diferencias a la regla general en tanto que estamos ante un caso de responsabilidad subjetiva o por culpa, concordante con el régimen general de responsabilidad de nuestro ordenamiento jurídico.

Ahora bien, es importante referirnos a las ideas detrás del sistema de responsabilidad civil extracontractual, para plantear una respuesta a si es que efectivamente la falta de tratamiento de las medidas de seguridad en nuestro ordenamiento jurídico supone su no adopción y que ellas no se encuentren implicadas en el artículo 11° de la LPD. En este sentido, es importante hacer alusión a la idea detrás del estándar de conducta.

A su respecto, en nuestro ordenamiento jurídico la noción de culpa del Código Civil se definiría en el Título Preliminar, incluyéndola entre “las palabras de uso frecuente en las

leyes". A su respecto, el artículo 44°[121] asume la clasificación tripartita de la culpa, dividiéndola en culpa grave, leve y levísima, que provenía del derecho romano[122].

Derivado del concepto de culpa presentado por este artículo se ha seguido que el estándar general y supletorio para el actuar corriente de las personas en la sociedad es la culpa leve, siendo el comportamiento que seguiría una persona normalmente diligente, que se caracterizaría por emplear un cuidado ordinario o razonablemente mediado. En ese sentido, el patrón de conducta que en condiciones normales se esperaría es el de una persona razonable y diligente, siendo ello a lo que se correspondería la idea del "buen padre de familia"[123].

Esta idea de "el actuar razonablemente esperable" o "normalmente diligente" de la conducta de un individuo es determinante a la hora de discernir si una persona afectada por un daño derivado de esta acción debe soportarlo o si, por contrario, debe indemnizar quien efectúo la conducta sin el cuidado naturalmente esperado. Ante este nivel de cuidado exigible lo que se busca es comparar la conducta realizada con la que puede esperarse, en las circunstancias del caso, de quien es normalmente respetuoso de los demás de forma común dentro de la vida en sociedad[124].

En añadidura, el concepto jurídico de negligencia hace referencia a la inobservancia de las exigencias típicas y objetivas de cuidado que debemos observar en nuestra vida diaria. Entendido de tal forma, podríamos decir que consistiría en requerimientos típicos porque están referidos a estándares de conducta que debemos observar en los diversos tipos de situaciones en que interactuamos dentro de la vida en sociedad. A su vez, serían objetivas, porque no atienden a las características particulares de cada miembro del grupo social, sino a un modelo de conducta. Siguiendo esta concepción, la culpa o negligencia puede ser concebida como *la inobservancia del cuidado debido en la conducta susceptible de causar*

[121] Artículo 44°: "*La ley distingue tres especies de culpa o descuido.*
Culpa grave, negligencia grave, culpa lata, es la que consiste en no manejar los negocios ajenos con aquel cuidado que aun las personas negligentes y de poca prudencia suelen emplear en sus negocios propios. Esta culpa en materias civiles equivale al dolo.
Culpa leve, descuido leve, descuido ligero, es la falta de aquella diligencia y cuidado que los hombres emplean ordinariamente en sus negocios propios. Culpa o descuido, sin otra calificación, significa culpa o descuido leve. Esta especie de culpa se opone a la diligencia o cuidado ordinario o mediano.
El que debe administrar un negocio como un buen padre de familia es responsable de esta especie de culpa.
Culpa o descuido levísimo es la falta de aquella esmerada diligencia que un hombre juicioso emplea en la administración de sus negocios importantes. Esta especie de culpa se opone a la suma diligencia o cuidado.
El dolo consiste en la intención positiva de inferir injuria a la persona o propiedad de otro".
[122] BARROS, Enrique. 2010. Tratado de responsabilidad extracontractual. Santiago, Editorial Jurídica de Chile. 80p.
[123] *Ibid.*, 81-82pp.
[124] *Loc. cit.*

daño a otros[125]. En este sentido, la culpa civil sería un juicio de ilicitud acerca de la conducta y no respecto de un estado de ánimo.

De esta idea se puede seguir que en el derecho civil la culpa tendría un doble aspecto. Por una parte, es un requisito que expresaría el principio de responsabilidad personal, porque se responde de los daños atribuibles a una conducta que contraviene un deber de cuidado, de modo que la obligación indemnizatoria sólo nace si el demandado ha incurrido en un comportamiento indebido a los ojos de nuestro ordenamiento jurídico. Por otra parte, la imputación de la negligencia es objetiva, con la consecuencia de que el juicio de disvalor no recae en el sujeto, sino en su conducta efectivamente realizada, de modo que resultarían irrelevantes las peculiaridades subjetivas del agente. Así, en consecuencia, el juicio civil de culpabilidad no corresponde a un reproche moral al autor del daño, sino un criterio jurídico para hacerlo responsable de las consecuencias dañosas de su acción[126].

Ahora, lo principal a revisar es cómo opera la seguridad de datos en el ámbito de la responsabilidad civil, particularmente las implicancias prácticas que tiene hoy en día la actual redacción del artículo 11 de la LPD.

Tal como se ha podido visualizar, la redacción del artículo 11 de la LPD es muy limitada a la hora de manifestar el contenido del principio de seguridad, al punto que ni siquiera indica qué es o implica el principio de seguridad, sino que, de la interpretación doctrinaria, de la propia historia de la ley y del entendimiento que se le ha dado en la práctica se ha concluido que se encuentra en dicha norma. En ese sentido, el principal problema que se ha podido encontrar en nuestra legislación es que no especifica medidas con las que el responsable cumpliría, en principio, con la debida diligencia en el cuidado de los datos, siendo este defecto comúnmente criticado por la doctrina y por los mismos legisladores, tal como presentamos en el capítulo anterior. A su respecto, podríamos concluir que nuestra legislación de datos tiene el principio de seguridad, con la salvedad de que nuestro legislador no ha incorporado medidas concretas para satisfacerlo ni ha esbozado algún acercamiento a este concepto en forma específica, lo cual es común en el ámbito comparado y que ha permitido concretizar el cuidado de los datos personales en otros países.

[125] *Ibid*., 77-78pp.
[126] *Loc. cit*.

A su respecto, bajo nuestra interpretación de dicha norma y que estimamos la pertinente para entender efectivamente incorporado el principio de seguridad de datos en nuestra legislación, cuando el legislador hace referencia al "cuidar los datos con la debida diligencia" nos indica que existe un estándar de conducta que se satisface o cumple al proteger la información personal que el responsable de datos tiene bajo su poder de forma normalmente cuidadosa, debiendo en este sentido adoptar las medidas de seguridad idealmente pertinentes que permitan garantizar su integridad, confidencialidad e indisponibilidad ante accesos indeseados. La no implementación del debido cuidado al proteger los datos llevaría a que el responsable infrinja el artículo en comento y, ante la existencia de daños, el titular de datos afectado pueda entablar la acción de indemnización de perjuicios del artículo 23° del mismo cuerpo normativo.

En este sentido, lo que debemos realizar para darle una funcionalidad práctica ha dicha norma y que finalmente sea operativo y no una mera declaración es ir a las ideas principales de la responsabilidad civil extracontractual, en particular lo que enunciamos respecto de la idea detrás del estándar de cuidado que sería la culpa. A su respecto, el no tener un catálogo específico de medidas de seguridad, las formas de su adopción y/o sus requisitos de cumplimiento no obstan a que podamos aplicarlas en nuestro país y hacerlas exigibles por medio del artículo 11 de la LPD, ya que será el juez quien *ex post* deberán definir cuándo se han adoptado las medidas apropiadas para el cumplimiento satisfactorio de este cuidado impuesto al responsable del banco de datos, comparando el estándar que nos entrega la norma con la conducta efectivamente desplegada, y verificando en el caso concreto si ello satisface o no lo que nos pide el legislador.

En otras palabras, lo que se debe realizar es aplicar este juicio normativo de responsabilidad y comparar el parámetro de conducta que nos entrega el legislador de datos con la conducta que en concreto realizó el responsable de datos. Es decir, para saber si yo como responsable adopté o no la debida diligencia en el cuidado de los datos, se debe realizar el mismo examen descrito en materia de responsabilidad civil extracontractual, buscando saber si en una misma situación, observando lo que comúnmente los miembros de la práctica harían en dicha circunstancia, se haya actuado diligentemente a efectos de proteger los datos que se encuentran en su poder y propender a su cuidado, comparándose así un modelo con lo que efectivamente se realizó.

Nuestro legislador al hablar de debida diligencia en materia de seguridad de datos nos está entregando un estándar de conducta que debiese de ser satisfecho adoptando una serie de medidas que tiendan a la protección de la información personal que está en manos del responsable. Cuáles o cómo debiesen de haber sido adoptadas para la satisfacción del estándar es una cuestión que se juega con posterioridad y que se verificará en sede jurisdiccional. En este sentido, la falta de tratamiento detallado del principio de seguridad no será óbice a que deban observarse medidas de seguridad para satisfacer la debida diligencia que el artículo 11° de la LPD nos entrega, ya que lo importante es entender que el deber de diligencia indicado en dicha norma, de su interpretación armónica con las distintas disposiciones de la LPD y entendiendo a dicho cuerpo normativo como uno que busca asegurar la protección de las personas y buscando el equilibrio de intereses entre titular y responsable, es que el principio de seguridad de datos se encuentra en la legislación y la debida diligencia en el cuidado de los datos supone la observancia de lo que nos pide este principio. A nuestro juicio no es realmente un problema en sede de responsabilidad civil que no exista la especificidad de tratamiento del principio de seguridad que sí se le da en otras legislaciones, ya que como indicamos lo importante es entender este deber de diligencia que se nos entrega en el artículo 11° a la luz del principio de seguridad y compararlo con la acción efectivamente realiza, siendo allí en donde verificaremos si efectivamente de cuidaron los datos con la debida diligencia.

Este planteamiento se hace necesario para poder darle una bajada concreta al principio de seguridad de datos y hacerlo cobrar sentido en nuestro país, ya que de otra forma únicamente se convertiría en un planteamiento vacío de nuestro legislador que no tiene un efectivo impacto en la vida real. Y, además, nos es necesariamente lógico, ya que al encontrarse dentro de nuestro ordenamiento el principio de seguridad, entendiéndose incorporado precisamente en el artículo mencionado, es que cuando nuestro legislador nos habla de la debida diligencia nos está hablando de un estándar de conducta que se debiese satisfacer adoptando las medidas que busquen la seguridad de la información personal, obedeciendo al concepto que implica el principio de seguridad.

Precisamente, a nuestro juicio el problema de la no especificidad dada por la ley respecto de en qué consisten las medidas de seguridad adoptables por el responsable de datos es más bien un cuestionamiento que apuntaría a otras áreas del ordenamiento jurídico en específico y no en materia de responsabilidad civil extracontractual. En este sentido, el estándar que se nos otorga hoy en día por parte de nuestro ordenamiento de datos en

materia de seguridad de datos no adquiere un carácter rígido y específico, funcionando como una lista que punto por punto se debe ir cumpliendo, sino que es suficientemente flexible para atender en concreto a las circunstancias externas de la acción, teniendo precisamente la ventaja de la adaptabilidad a las circunstancias del caso, tal como lo plantea el profesor Barros a la hora de referirse a la culpa como estándar de cuidado[127]. Así, serán nuestros Tribunales de Justicia quienes caso a caso deberán de ir identificando si se cumplió o no con el cuidado diligente de los datos, pudiendo concluir que sería más bien una construcción casuística y con posterioridad a la perpetración de los hechos que acarrearían la responsabilidad.

Si es que existiera una determinación de las medidas de seguridad que sea rígida y/o lo suficientemente específica para operar como una suerte de "lista de chequeo", nuestro responsable de datos le daría satisfacción al estándar de conducta que se le es exigible una vez vaya, punto por punto, cumpliendo con las exigencias normativas particulares y verificándose prácticamente de inmediato ello. Este no sería el caso de nuestro país, en tanto que al no existir entre tratamiento pormenorizado que se ha advertido, lo que ocurre es que el deber de diligencia que nos pide el artículo 11° se caracterizaría por ser más abierto, interpretando que su contenido se forma en base a las ideas basales detrás del principio de seguridad, pero no circunscrito a una o más formas específicas de adoptarlo.

Poniéndolo en un ejemplo práctico, nuestro responsable de datos no satisface el estándar de cuidado implementando tal o cual tipo específico de software para proteger sus sistemas informáticos, ni capacitando de maneras particulares a sus trabajadores, ni tampoco adoptando medidas organizativas internas específicas con encargados especializados en la seguridad de la información personal (todas cuestiones que se han podido ir vislumbrando en el ámbito comparado), sino que lo que haremos será construir el estándar con posterioridad, llevándonos a comparar la conducta efectiva con el actuar que es posible exigirse de forma razonable[128]. Siendo esto, a la luz del artículo 11° de la LPD, si es que las medidas que se hayan adoptado para cuidar los datos personales son apropiadas, en condiciones similares y bajo un comportamiento normalmente razonable de los individuos que participan en dicha actividad, para el cuidado diligente de los datos.

[127]BARROS. E. 2005. La Culpa en la Responsabilidad Civil. Ensayos Jurídicos Universidad Alberto Hurtado. Santiago, Publicaciones Escuela de Derecho Universidad Alberto Hurtado. 8p.
[128] *Loc. cit.*

Es acá en donde no nos encontramos completamente de acuerdo con la doctrina nacional al identificar problemas con en el principio de seguridad de datos y la no especificación de las medidas de seguridad y sus implicancias, ya que, si bien diversos autores advierten lo limitado y escueto de este principio en nuestro país, suelen tratarlo más bien en atención a la autoridad de control en materia de protección de datos y no en mira a la eventual responsabilidad civil. Por ejemplo, indican que el cumplimiento y ejecución concreta de las medidas de seguridad necesarias por parte del responsable del banco de datos deben ser fiscalizados por la autoridad[129], pero esta labor vendría a ser más bien una cuestión idealmente previa si es que lo tomamos como un control preventivo de la labor de tratamiento de datos y a la vez represiva, a la hora de sancionar administrativamente al responsable que no cumplió con las exigencias normativas respectivas de su actividad, pero ello no supone que el titular de datos hoy en día, con nuestra LPD, no tenga una herramienta para exigir una reparación ante la inobservancia de adoptar medidas de seguridad. La realidad nacional es que no tenemos, hoy en día, una autoridad de control de datos como tal que verifique este cumplimiento, lo cual no impide que, en sede de justicia ordinaria, en base a las reglas entregadas por nuestro ordenamiento, se pueda perseguir la responsabilidad civil de la persona encargada del tratamiento de datos.

En este sentido, podría argumentarse que no serían exigibles las medidas de seguridad en sede civil, en el entendido de que no hay autoridad de control en nuestro país que persiga su debido cumplimiento y adopción. No obstante, este argumento es erróneo, en tanto que, en un primer punto, los fundamentos de la responsabilidad civil son distintos de los de un régimen sancionatorio por parte de la administración. Una cosa es el *compliance* de datos personales, mientras que otra muy distinta es el juicio de responsabilidad civil, ya que, para este último, en sus fundamentos más primigenios, lo primordial a lo que alude es que una persona no deba soportar el daño que sufrió derivado de una conducta imputable a la culpa o dolo de otra. De ello, es que en la práctica la no adopción de medidas de seguridad puede conllevar una indemnización de los perjuicios derivados de la inobservancia del debido cuidado de los datos, ya que es una conducta que se espera y de la que el legislador indica que se es responsable civilmente, no debiendo un titular de datos soportar un daño derivado de la infracción al deber de seguridad del artículo 11° de la LPD.

[129] CERDA, A., *Op. Cit.*, 26p.

Esto último, es muy diferente al cumplimiento de las disposiciones que acarrean sanción administrativa en el derecho comparado, ya que en esta sede, primordialmente, lo que se busca es la licitud de la actividad económica (o también administrativa, en el caso de un órgano público), estableciéndose los requerimientos que se deben tener, por ejemplo, empresarialmente, para que se cumpla con la normativa de protección de datos, en tanto que ella funciona como norma que regula la actividad en sí respecto del orden público y la protección de los derechos de las personas.

Como añadidura al planteamiento del control posterior que realizan los tribunales, podríamos indicar analógicamente lo que ocurre en materia de Derecho del Trabajo. Si bien acá no hablamos de datos y el desarrollo de la norma es más detallado, el artículo 184 del Código del Trabajo[130] habla de las medidas que debe adoptar el empleador para cuidar la vida y salud de sus trabajadores. Esta norma no tiene un catálogo detallado y específico que encause con precisión de lo que se habla cuando se refiere a estas medidas y, a juicio de Gajardo, esta obligación de cuidado sería más bien carácter dinámico, que cambia en base a las formas de realizar el trabajo, a los avances tecnológicos, al marco regulatorio en que se desenvuelve la actividad económica del empleador. Así, las distintas circunstancias que van modificando la actividad implican un cambio en la manera de prevenir los riesgos que se van generando y, en consecuencia, en las formas en que se le da cumplimiento[131].

Si bien, como indicamos estamos hablando de campos distintos y que en materia de protección de datos se nos entrega de forma mucho más limitada, lo que buscamos con la analogía es plantear que la práctica jurisprudencial[132] de este deber de seguridad en materia laboral precisamente se va satisfaciendo caso a caso, no existiendo un catálogo por parte del legislador en donde se enuncien las medidas de protección que específicamente se deben de ir adoptando por parte del empleador para satisfacer el deber, sino que se propende a analizar *ex post* el caso particular, comparándolo con un modelo de empleador normalmente cuidadoso, que en similares condiciones hubiese adoptado las medidas necesarias para asegurar la protección de sus trabajadores y, si la acción perpetrada efectivamente no resiste esta comparación, el empleador sería responsable.

---

[130] Artículo 184, inciso primero: "*el empleador estará obligado a tomar todas las medidas necesarias para proteger eficazmente la vida y salud de los trabajadores, informando de los posibles riesgos y manteniendo las condiciones adecuadas de higiene y seguridad en las faenas, como también los implementos necesarios para prevenir accidentes y enfermedades profesionales*".

[131] GAJARDO, M. C. 2014. El Deber de Seguridad. En: Revista Chilena de Derecho del Trabajo y de la Seguridad Social 5(9): 22p.

[132] Ejemplos pueden ser las sentencias rol N°3495-2010 de la Corte Suprema y rol N° 158-2010 de la Corte de Apelaciones de Concepción.

En definitiva, a lo que queremos apuntar con este apartado es que lo fundamental para poder darle una bajada concreta al principio de seguridad y darle efectividad a su adopción es ir al juicio normativo de responsabilidad y entender la operación que se realiza para discernir si se cumple o no con un deber de conducta. A este respecto, nuestro ordenamiento de datos en el artículo 11 de la LPD nos entrega un deber de conducta que es la debida diligencia en el cuidado de los datos, el cual se satisface cuando, precisamente a la luz del principio de seguridad, el responsable adopte las medidas que propendan a la protección de los datos que tiene en su poder. En este sentido, la determinación de si existió una satisfacción o no del estándar quedará entregada a la labor del juez, quien comparará las acciones en concreto del responsable con aquello que, en una misma situación, en base a lo que comúnmente los miembros de la práctica harían en dichas circunstancias, se debiese de haber realizado.

2. LA RELACIÓN CON LA AUTORIDAD DE CONTROL Y LA MITIGACIÓN DE DAÑOS

Como comentario aparte a lo anteriormente expuesto, estimamos importante para un análisis más acabo de la seguridad de datos personales lo relevante de la autoridad de control de datos y su relación con la posibilidad de mitigar posibles daños que pueda sufrir la víctima.

Tal como indicamos, en Chile hoy no tenemos una autoridad de control de datos como sí ocurre en otros países con marcos regulatorios más robustos, como puede ser el caso de España. En dicho país europeo, la Agencia Española de Protección de datos es muy activa a la hora de cumplir su rol y no centra su esfuerzo únicamente en verificar el cumplimiento a la normativa de protección de datos personales y sancionar cuando corresponda, sino que también tiene un rol educador muy importante, elaborando guías y estudios para que las personas conozcan sus derechos y sea de común entendimiento el marco regulatorio de la protección de datos.

En este sentido, una relevante diferencia y que puede influir en materia de daños es que en Chile no existe una obligación de reporte de brechas de seguridad de datos en la LPD, lo que implica que el titular muchas veces no tenga conocimiento de que se tuvo acceso a su información personal o que esta fue filtrada. Cuestión que sí ocurre en el caso

español, estando su autoridad de control de datos facultada para sancionar en caso de que no se cumplan las respectivas imposiciones legales[133].

De esta manera, el titular de datos no podría adoptar las medidas necesarias tendientes a mitigar, total o parcialmente, los posibles daños (tanto moral como patrimonial) que pueda sufrir derivados de la filtración de su información.

No solo ello aporta a la mitigación de los posibles daños, puesto que, sin la existencia de una autoridad de control, no existe tampoco la efectiva coordinación entre responsable y autoridades administrativas para hacer frente a problemas de seguridad de datos En este sentido, si se tiene conocimiento de este tipo de incidentes, pueden darse respuestas coordinadas entre responsable y autoridades, que permitan mitigar los daños derivados de ellos y facilitar la recuperación del control, disponibilidad e integridad de la información personal.

Este deber de reporte de incidencias de seguridad de datos, tal como indicamos en el apartado de derecho comparado, se encuentra presente en otros ordenamientos jurídicos y necesariamente viene acompañado de regímenes sancionatorios para el responsable que no cumpla con ello.

Desde un punto de vista económico, la existencia de sanción es muy importante, ya que genera los incentivos para que efectivamente se reporte y se pueda responder a la incidencia. De no tener las debidas sanciones, es muy dable que el responsable prefiera no reportar e intentar solucionar por su cuenta (o incluso intentado que pase desapercibida) la problemática, ya que puede con el problema de seguridad de datos puede proyectar una mala imagen al mercado. Es decir, que el balance entre lo costoso de la sanción y las posibles repercusiones que pueda tener que el mercado sepa de la situación, debiese ir cargado hacia la primera, ya que así se estarían generando los incentivos suficientes para promover el reporte.

A la vez, en nuestra legislación no existe un tratamiento detallado y expreso de las transferencias internacionales de datos, las cuales son de una importante relevancia a la hora de verificar la seguridad de la información, ya que en el ámbito comparado

[133] De hecho, es tal la preocupación a este respecto, que en la propia página web de la Agencia Española de Protección de Datos existe una guía de su autoría para ayudar al responsable con todo lo relativo al reporte de brechas de seguridad. En este sentido, véase: AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. 2018. Guía para la gestión y notificación de brechas de seguridad. [en línea] <https://www.aepd.es/guias/index.html> [consulta: 11 de enero de 2019]

comúnmente se entiende que, al país al que se transfiere, debe de tener un ámbito de protección de datos adecuado, lo que incluiría, precisamente, que existan medidas de seguridad por parte de los responsables de datos[134].

3. MODIFICACIONES A LA NORMATIVA DE SEGURIDAD DE DATOS

Finalmente, para cerrar el análisis de la seguridad de datos planteado en este capítulo, analizaremos las principales modificaciones normativas que se han ido dando, así como las que se encaminan para cambiar la actual regulación de la seguridad de datos en nuestro país. En este sentido, haremos mención de la normativa sectorial de seguridad informática bancaria de la Superintendencia de Bancos e Instituciones Financieras (SBIF) y el proyecto de ley de datos personales que actualmente se discute en el Senado.

- Normativa sectorial de la SBIF

El año 2018, sin duda, fue uno de los años más relevantes para la ciberseguridad en nuestro país. Esto se debe principalmente a la seguidilla de casos de robos a bancos de nuestro país por parte de hackers, siendo el más destacable el caso del Banco de Chile, que perdió cerca de diez millones de dólares por parte de hackers de Corea del Norte, acaecido a finales de mayo[135].

A raíz de estas situaciones, las autoridades chilenas no se mantuvieron al margen y en materia de ciberseguridad se realizaron una serie de medidas tendientes a mejorar el marco

---

[134] En este sentido, el GDPR indicada en su considerando 101° que: "*Los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacionales. El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal. No obstante, si los datos personales se transfieren de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión por el presente Reglamento, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional. En todo caso, las transferencias a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena conformidad con el presente Reglamento. Una transferencia solo podría tener lugar si, a reserva de las demás disposiciones del presente Reglamento, el responsable o encargado cumple las disposiciones del presente Reglamento relativas a la transferencia de datos personales a terceros países u organizaciones internacionales*".
De igual forma esta exigencia de adecuación es tratada a lo largo del reglamento y principalmente en su Capítulo V "Transferencias de datos personales a terceros países u organizaciones internacionales". Acá existe un tratamiento orgánico de las exigencias que se deben cumplir para la transferencia de datos a terceros países, siendo la exigencia principal el que la transferencia no suponga una limitación o menoscabo de los derechos de los titulares. De ello se desprende que un ejemplo de una limitación o menoscabo de estos derechos es la transferencia a un país que no tenga un deber de adopción de medidas de seguridad, no teniendo el principio de seguridad de datos incluido en su legislación, ya que ello conllevaría que no se encuentra presente una exigencia de cuidado sobre los datos por parte del responsable.

[135] Para más información respecto de la situación de la ciberseguridad en nuestro país durante 2018, véase: <https://www.latercera.com/pulso/noticia/ciberseguridad-los-desafios-los-reguladores-2019/472866/#> [consulta:11 de enero 2019]

normativo existente al respecto en nuestro país, destacando en esta materia el envío al Congreso de un proyecto de nueva ley de delitos informáticos (boletín N°12.192-25, actualmente en su primer trámite constitucional), el cual viene a modificar la actual "Ley de Delitos Informáticos" (Ley N°19.223) que data de 1999 y que se encuentra en una manifiesta anacronía respecto de nuestra actual realidad en el ciberespacio y las tecnologías de la información.

Por su parte, desde la regulación del sector bancario y financiero tampoco se quedaron al margen y proliferaron una serie de normativas por parte de la SBIF que buscaban regular para las instituciones de este sector de la actividad económica temas relativos a la ciberseguridad, principalmente respecto a la consideración de este factor de riesgo en el negocio, así como la notificación de problemas de ciberseguridad a esta superintendencia.

En específico, se modificaron los capítulos 1-13 y 20-8 de la Recopilación Actualizada de Normas (RAN) de la SBIF, que es un conjunto de normativa sectorial agrupada según temas específicos y que está destinada a la regulación del ámbito bancario y financiero.

El capítulo 1-13 de la RAN, titulado "Clasificación de gestión y solvencia", contiene una serie de disposiciones tendientes a dar cumplimiento a lo indicado en el Título V de la Ley General de Bancos[136], que en su articulado mandata a la SBIF a mantener, permanentemente, la clasificación de gestión y solvencia de los bancos e instituciones financieras, conforme al procedimiento señalado en dicho título (artículos 59° y siguientes).

En resumidas cuentas, lo que trata esta norma es la categorización de las instituciones a las que se refiere en base a su capacidad de gestión y la solvencia que tengan, conllevando una serie de consecuencias el encontrarse en una u otra categoría. Para esta clasificación se tienen en consideración diferentes puntos de evaluación que la SBIF califica para ubicar a determinada entidad en uno u otro nivel, entre los que podemos destacar el correcto gobierno corporativo, así como la capacidad de administración y control de los diferentes riesgos de la actividad (como pueden ser el riesgo de crédito, financiero y el riesgo operacional).

La modificación a este capítulo apuntó a la consideración de los problemas de ciberseguridad, como terminología específica, dentro de los riesgos para tener en cuenta

[136] Chile. Ministerio de Hacienda. 1997. Decreto con Fuerza de Ley 3: Fija texto refundido, sistematizado y concordado de la Ley General/ de Bancos y de otros cuerpos legales que se indican. 19 de diciembre 1997.

por los responsables de la institución bancaria y que son de relevancia para la clasificación realizada por la SBIF. En ese sentido, la normativa se dirige a la búsqueda de una adecuada gestión de la infraestructura crítica de las instituciones bajo la supervigilancia de esta superintendencia, en materia de cibserseguridad.

De esta forma, se apunta a que el Directorio de las instituciones debe preocuparse de identificar la infraestructura crítica en términos de ciberseguridad, lo que incluye los activos de información lógicos que son considerados críticos para el funcionamiento del negocio y del sistema financiero en su conjunto. A su vez, se entiende que son parte de esta infraestructura los componentes físicos, como el hardware que se posee y los sistemas tecnológicos de almacenamiento, administración y soporte de activos, los cuales, de no operar adecuadamente, exponen a la entidad a riesgos de integridad, disponibilidad y confidencialidad de la información.

De igual forma, es muy destacable el esfuerzo realizado por la SBIF en este apartado de la normativa en comento, ya que el Anexo N°3 presenta una definición de ciberseguridad para efectos de esta sección, cuestión que no se encuentra presente, hoy en día, en la legislación nacional. En específico, indica que "*Ciberseguridad es un concepto que comprende al conjunto de acciones para la protección de la información presente en el ciberespacio, así como de la infraestructura que la soporta, que tiene por objeto evitar o mitigar los efectos adversos de sus riesgos y amenazas inherentes, sobre la seguridad de la información y la continuidad del negocio de la institución*"[137].

Lo anterior es del todo interesante para la seguridad de datos personales ya que, sin ánimo de realizar un profundo desarrollo, es muy importante destacar su relevante relación con la ciberseguridad, debido a que esta última supone un conjunto de acciones que conllevan, directa o indirectamente, el cuidado de los datos. En ese sentido, si un responsable de datos, que en este caso es un banco, toma las medidas para asegurar la ciberseguridad en su actividad, estaría conllevando seguridad de datos personales también[138].

[137] Superintendencia de Bancos e Instituciones Financieras. Última versión de 2018. Capítulo 1-13 de la Recopilación Actualizada de Normas. [en línea] <https://www.sbif.cl/sbifweb/servlet/LeyNorma?indice=3.1.2&LNAN=1> [consulta: 04 de enero de 2019]

[138] Con todo, es importante realizar una diferenciación. A nuestro juicio es bastante correcta la definición de ciberseguridad que realiza la SBIF y del concepto podemos desprender que la seguridad de datos se podría encuadrar dentro de la ciberseguridad. Esto queda mejor ilustrado al ejemplificar con un banco que adopta las medidas necesarias para resguardar el riesgo de ciberseguridad en su negocio. Al hacerlo, esta institución podría estar protegiendo, entre otras cosas sus fondos, su información confidencial, claves dentro utilizadas

Por otro lado, también tenemos el Capítulo 20-8 de la RAN, que a nuestro juicio es el más destacable de los dos. Éste tiene por título "Información de incidentes operacionales", y su objeto es el establecimiento de requisitos relativos a la información que se debe enviar a la SBIF cuando ocurran incidentes operacionales, existiendo la imposición a las entidades de mantener en conocimiento a dicha superintendencia respecto de los incidentes que puedan afectar o colocar en riesgo la continuidad del negocio, los fondos o recursos de la entidad o sus clientes, así como la calidad o la imagen de la institución. La particularidad de la modificación al efecto fue que, dentro de los incidentes operacionales a informar, se incluyó específicamente aquellos en materia de ciberseguridad.

Pero no limitado a ello, es tal la importancia que los incidentes de ciberseguridad han adquirido en esta industria, que no sólo se debe comunicar a la SBIF, sino que también deben de ser compartidos por la institución al resto de los actores del sector, a modo de proteger a los usuarios y al sistema en su conjunto. Así, el principal objetivo de dicho mecanismo es prevenir a los participantes de la industria bancaria sobre las amenazas de ciberseguridad, permitiendo que el resto de las entidades tome los resguardos necesarios para lograr la detección, respuesta y recuperación, y así conseguir disminuir la probabilidad de que las consecuencias negativas de un problema de ciberseguridad se propaguen por todo el sistema bancario nacional[139].

En este capítulo de la RAN se establece que la información debe ser enviada mediante una casilla específica habilitada por la SBIF, en el plazo de treinta minutos luego de su ocurrencia. Para ello, la entidad deberá definir un funcionario encargado, quien realizará los reportes y enviará la información, debiendo tener un nivel ejecutivo dentro de la organización y ser designado por la institución bancaria tanto para esta labor de reporte, como para responder eventualidad consultas por la SBIF.

En específico la normativa diferencia la información a reportar en el inicio del incidente, de la que se reporta al momento del cierre del incidente. Así entendido, se impone que en este reporte exista un mínimo de información que incluya los siguientes

---

dentro de su propia organización, entre otras; pero, a su vez, con estas medidas podría también estar protegiendo la información personal de sus clientes o trabajadores, lo que conllevaría seguridad de datos personales. Si, por ejemplo, mantiene diligentemente revisados los softwares antivirus que utiliza, teniéndolos actualizados y en correcto funcionamiento, así como teniendo trabajadores que procuren que esto ocurra, estaría tomando medidas que, lo más probable, es que protejan la información del banco y sus fondos, así como la información personal de sus clientes.

[139] En este sentido véase: Superintendencia de Bancos e Instituciones Financieras. Última versión de 2018. Capítulo 20-8 de la Recopilación Actualizada de Normas. 3p. [en línea] <https://www.sbif.cl/sbifweb/servlet/LeyNorma?indice=3.1.2&LNAN=1> [consulta: 04 de enero de 2019].

aspectos, diferenciando el reporte en momento preliminares del incidente, de los antecedentes enviados a su cierre, teniendo como principal diferencia la exactitud de la información[140]:

i. Al momento del inicio del incidente: número único identificador del incidente (asignado por la SBIF); nombre de la entidad informante; descripción del incidente; fecha y hora de inicio del incidente; causas posibles o identificadas; productos o servicios afectados; tipo y nombre de proveedor o tercero involucrado; tipo y número estimado de clientes afectados; dependencias y/o activos afectados; medidas adoptadas y en curso; otros antecedentes.

ii. Al momento del cierre del incidente: Número único identificador del incidente; nombre de la entidad informante; descripción del incidente; causas identificadas; fecha y hora de inicio del incidente; fecha de cierre del incidente; productos o servicios afectados; tipo y nombre de proveedor involucrado; tipo y número de clientes afectados, dependencias y/o activos afectados; medidas adoptadas; otros antecedentes.

A su vez, la norma indica que cuando se trate de incidentes que afecten la calidad o continuidad de los servicios a los clientes o se trate de un hecho de público conocimiento, la institución será responsable de informar oportunamente a los usuarios sobre la ocurrencia de dicho evento, debiendo actualizar la información disponible hasta el momento que el incidente se encuentre superado.

A nuestro juicio, esta es la novedad que particularmente celebramos, ya que estamos ante un caso de obligación de reporte de brechas de seguridad, que además tiene tres destinatarios por parte del banco: SBIF, resto de instituciones de la industria y, en determinados casos, los clientes. Esto permitiría solventar, en el sector bancario, el problema que identificamos en relación con la mitigación de daños luego de una brecha de seguridad, ya que permite que el titular se encuentro en conocimiento y tome las medidas que estime necesarias para protegerse de posibles daños derivados de la filtración de su información personales al existir un incidente de ciberseguridad.

Con todo, pensamos que lo ideal en este aspecto es que se encuentre tratado de manera general en la LPD (y que pasaremos a ver en relación con el proyecto de ley al respecto) o

[140] *Ibid.*, 2-3pp.

en una ley específica que mandate que todo responsable deba informar de la brecha de seguridad de datos y no únicamente reducido a este sector industrial específico.

- Proyecto de ley de datos personales

Ahora bien, sin dudas el proyecto de ley más importante para esta área de estudio es el proyecto de ley que "regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales" (boletines N°11.144-07 y 11.092-07, refundidos), comúnmente denominado "proyecto de ley de datos personales". Este proyecto es un refundido de la moción elaborada por los Senadores Harboe, Araya, De Urresti, Espina y Larraín (boletín N°11.092-07), con el mensaje elaborado en el segundo gobierno de Michelle Bachelet (boletín N°11.144-07).

Se trata de una reforma integral al marco regulatorio de los datos personales en nuestro país, buscando actualizar y mejorar nuestra LPD, haciéndose cargo de las falencias que se han ido identificado la doctrina y la jurisprudencia con los años. De esta forma, este proyecto trata, entre otros temas: el alcance de dato personal; regula con mayor detalle los requisitos del consentimiento del titular de datos; diferencia conceptualmente distintas categorías especiales de datos personales; establece y regula de forma expresa los derechos de los titulares y los principios de la normativa; crea una autoridad de control de datos personales, con el nombre de "Agencia de Protección de Datos Personales"; regula específicamente las transferencias internacionales de datos personales; establece un régimen sancionatorio particular; entre varios puntos.

Actualmente este proyecto de ley se encuentra en su primer trámite constitucional en el Senado, esperándose el inicio de la discusión de las indicaciones presentadas por parte del Ejecutivo y otros parlamentarios.

Para efectos de este trabajo, el principal punto a destacar es que este proyecto se hace cargo de las falencias que la seguridad de datos personales tiene en la actual LPD. Como primer punto a considerar es que, entre las pretensiones que tiene, busca establecer el catálogo de principios que tendrá la ley, entre los cuales se encuentra el principio de seguridad.

De esta forma, en la letra f) del pretendido nuevo artículo 3°, se establece que el principio de seguridad conlleva que "*en el tratamiento de los datos personales, el responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el*

tratamiento no autorizado, pérdida, filtración, daño o destrucción y, aplicando para ello, las medidas técnicas u organizativas apropiadas".

Al tenor del pretendido texto legal podemos desprender que se define el principio de seguridad, precisamente, conllevando una garantía de cuidado de los datos, lo que supone la adopción de medidas adecuadas por parte del responsable. En ese sentido, se pretende volver explícita la imposición legal del deber de adopción de medidas de seguridad.

A su vez, dedica un artículo específico a la obligación de adoptar medidas de seguridad, imponiendo que el responsable de datos debe adoptar las medidas necesarias para resguardar el cumplimiento del principio de seguridad establecido en la ley considerando el estado actual de la técnica y los costos de aplicación, junto con la naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados. Igualmente, indica que las medidas aplicadas por el responsable deben asegurar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos (artículo 14° quáter).

De igual manera, indica que, si las bases de datos que opera el responsable tienen distintos niveles de criticidad, el responsable deberá adoptar las medidas de seguridad que correspondan al nivel más alto. Y, de ocurrir un incidente de seguridad, en caso de controversia judicial o administrativa, corresponderá al responsable acreditar la existencia y el funcionamiento de las medidas de seguridad adoptadas en base a los niveles de criticidad y a la tecnología disponible.

Finalmente, también destacamos a este respecto que este proyecto de ley busca establecer una obligación de reporte de vulneraciones a las medidas de seguridad de datos adoptadas, indicando que el responsable de datos deberá reportar a la Agencia de Protección de Datos Personales, por los medios más expeditos posibles y sin dilaciones indebidas, estas vulneraciones que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate, así como la comunicación o acceso no autorizados a dichos datos, cuando exista un riesgo razonable de que con la vulneración se genere un perjuicio o afectación para los titulares de datos.

Respecto a la comunicación, pretende establecer algo similar a lo que se indica en el Capítulo 20-8 de la RAN, imponiéndole al responsable de datos que deberá registrar estas comunicaciones con la autoridad de control, describiendo la naturaleza de las

vulneraciones sufridas, sus efectos, las categorías de datos y el número aproximado de titulares afectados y las medidas adoptadas para gestionarlas y precaver incidentes futuros. De igual manera, se hace cargo en este aspecto de los diversos tipos de datos personales e indica que cuando dichas vulneraciones se refieran a datos personales sensibles o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, el responsable deberá también efectuar esta comunicación a los titulares de estos datos. Esta comunicación deberá realizarse en un lenguaje claro y sencillo, singularizando los datos afectados, las posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo adoptadas. La notificación se deberá realizar a cada titular afectado y si ello no fuere posible, se realizará mediante la difusión o publicación de un aviso en un medio de comunicación social masivo y de alcance nacional (artículo 14° quinquies).

Como podemos visualizar, ya en su texto más primitivo, el proyecto de ley de datos personales se hace cargo de las problemáticas relativas a la seguridad de datos que se pueden identificar hoy en día en nuestra legislación, tratando orgánica y expresamente el deber de seguridad de datos y las medidas de seguridad, así como estableciendo una obligación de reporte de las vulneraciones a la seguridad de datos, debiendo comunicar a los titulares cuando corresponda.

A nuestro parecer, sin lugar a duda, este es un avance muy significativo en la materia, y esperamos con ansias que siga avanzando en el Congreso Nacional, a fin de tener una nueva y mejor LPD, cumpliendo con estándares internacionales y solventando las numerosas deficiencias que hoy en día se identifican en el marco regulatorio de la protección de datos personales en nuestro país.

CONCLUSIONES

Para cerrar este trabajo, quisiéramos hacer hincapié en algunas de las ideas más importantes que tratamos a lo largo de estas páginas. En ese sentido, partiremos aludiendo a las principales características que hemos identificado en la Ley N°19.628.

Primordialmente, nos encontramos ante una legislación que busca regular en forma general la protección de datos en nuestro país, estableciendo un marco regulatorio que busca conciliar el legítimo interés de aquellos que quieren trataran datos y sacar provecho de ello, como también el interés de las personas en controlar la información que les concierne y que se encuentra en poder de otros.

A su vez, las principales figuras de este marco normativo son el titular y el responsable de datos. Respecto de ello, no nos cabe duda de que los titulares de datos son, excluyentemente, las personas naturales, en base a la expresa definición que el legislador nos entrega en el artículo 2° letra ñ) del mencionado cuerpo legal, no siendo aplicable a las personas jurídicas. En contrapartida, el responsable puede ser tanto persona natural como jurídica, a la vez que independiente de que sea privado o público.

Por su parte, tenemos que tener en consideración la basta cantidad de temas que actualmente no son tratados en nuestra LPD, como puede ser a transferencia internacional de datos, la diferenciación entre categorías especiales de datos o una regulación más clara que nos permita diferenciar en la práctica, por ejemplo, el tratamiento de un dato sensible de otros datos. De ello, es que urge una modificación legislativa que nos brinde un marco normativo que esté acorde a la realidad de las tecnologías de información y del mercado de datos personales, siendo, a nuestro juicio, preocupantemente relevante la distancia de dos décadas entre la sociedad que originalmente buscó regular esta ley, con la que actualmente existe.

En lo que respecta al régimen de indemnización de perjuicios del artículo 23° de la LPD, es claro que estamos ante un régimen por culpa, según las reglas generales de nuestro sistema de responsabilidad civil. Dentro de este artículo hay que diferenciar el supuesto relativo a la tramitación de una acción de habeas data, de la acción ejercida en base a una infracción distinta a la LPD, como puede ser una infracción a su artículo11°, ya que el procedimiento a seguir será diferente entre uno y otro caso.

De igual forma, hay que destacar la opción que adoptó el legislador de establecer un procedimiento sumario para la tramitación de la acción de indemnización de perjuicios del artículo 23° ya que, a nuestro juicio, permite conseguir con mayor facilidad el objetivo de protección de derechos de las personas que tiene la LPD. Lo anterior, debido a que es una legislación que, precisamente, busca el resguardo de la capacidad de control que las personas tienen sobre su información personal, protegiéndoles de las posibles consecuencias dañinas que pudieren derivarse de la exposición de sus datos personales.

Ahora bien, en lo que respecta a la seguridad de datos, a nuestro juicio se hace claro que este principio se encuentra incorporado en nuestra legislación en el artículo 11°, lo que conlleva un deber de cuidado por parte del responsable sobre los datos, que en derecho comparado y en doctrina se entiende que se manifiesta en la adopción de medidas de seguridad de datos.

A nuestro juicio, si bien es claro lo escueta y quizá limitativa de la expresión "deberá cuidar de ellos con la debida diligencia" que está en el artículo 11° LPD y el poco tratamiento que se le da al principio de seguridad en nuestra legislación, eso no implica que el debido cuidado de los datos suponga la adopción de medidas de seguridad pertinentes y tendientes a la satisfacción de la norma. Esto es debido a que no es necesario un tratamiento pormenorizado y específicos de qué se entiende y/o qué se debiese de cumplir particularmente para satisfacer diligentemente un cuidado de los datos, ya que el criterio para discernir la suficiencia o no quedará en manos de nuestros Tribunales de Justicia, quienes a la hora de efectuar un juicio normativo de responsabilidad civil compararán la conducta efectuada por el responsable con el estándar de cuidado diligente de los datos y, si de dicha acción desplegada por el responsable no alcanza para satisfacerle, será responsable de los daños derivados.

Ofrecemos esta interpretación de la norma, ya que le permite dar sentido a que exista un principio de seguridad de datos en nuestra legislación, puesto que, sin existir la posibilidad de hacer responsable de su debida protección, al menos civilmente, a la persona encargada de los datos, no se debiese de entender la presencia de la seguridad de datos en nuestra LPD. Así, dicha interpretación sería la que permitiría que el principio de seguridad no sea una mera enunciación y finalmente se convierta en letra muerta en nuestro ordenamiento jurídico, haciendo prácticamente inoperante e irrelevante su incorporación en nuestro ordenamiento jurídico.

Finalmente, hay que destacar la importancia de este ítem hoy en día, ya que la información personal es de un altísimo valor. Nos movemos en una economía de datos y en una sociedad informatizada, lo que conlleva que sean un bien muy codiciado y, por tanto, que conlleven un riesgo claro de robo, pérdida, destrucción, entre otras, por lo que requieren ser resguardados cuidadosamente.

En este sentido, identificamos que existen manifiestas deficiencias en nuestra LPD en materia de seguridad de datos, siendo sumamente necesaria la presencia de una autoridad de control que sancione y ayude en la respuesta a las brechas de seguridad de datos, ya que ello permitiría mitigar, total o parcialmente, los daños que los titulares podrían sufrir por la filtración de su información personal. De ello, celebramos el gran avance que dio la SBIF en el año 2018, estableciendo para su sector económico una exigencia de reporte de brechas seguridad, así como esperamos con alta expectación el avance del proyecto de ley de datos en el Senado.

La protección de datos personales es un área del estudio jurídico que esencialmente no es muy novedosa, sino más bien que es muy desafiante, ya que se encuentra intrínsecamente relacionada con el constante avance del uso y de las capacidades de las tecnologías de la información en nuestra sociedad. Desde hace décadas que en las diferentes legislaciones a lo largo del mundo se han ido haciendo cargo de todo el campo de temas que envuelve la protección de datos y que han ido dando cuenta de la necesidad de regularla.

En este sentido, esperamos que este trabajo sea un humilde insumo para poder entender más sobre la regulación de la protección de datos en nuestro país y, específicamente, cuál es el deber de seguridad de datos, puesto que es uno de los temas más relevantes a discutir por nuestro parlamentarios en vista a una posible nueva ley de protección de datos, precisamente porque una de las cosas que se busca es robustecer nuestro marco normativo y garantizar los derechos de las personas respecto de su información personal, cuestión en que la debida seguridad de los datos personales es crucial para asegurar estos fines.

BIBLIOGRAFÍA

Bibliografía consultada

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. 2018. Guía para la gestión y notificación de brechas de seguridad. 56p. [en línea] <https://www.aepd.es/guias/index.html> [consulta: 11 de enero de 2019]

ANGUITA, P. 2007. La protección de datos Personales y el derecho a la vida privada. Régimen Jurídico, Jurisprudencia y Derecho Comparado: análisis de la Ley No. 19.628 sobre Protección de la Vida Privada (Protección de Datos de Carácter Personal), modificada por la Ley No. 19.812. Santiago, Editorial Jurídica de Chile. 627p.

ARRIETA, R. 2009. Chile y la Protección de datos personales: Compromisos internacionales. En: Chile y la protección de datos personales: ¿Están en crisis nuestros derechos fundamentales? Serie de Políticas Públicas. Santiago, Ediciones Universidad Diego Portales. pp. 13-22.

ARRIETA, R. 2011. Autorregulación y protección de datos personales. En: Reflexiones sobre el uso y abuso de los datos personales en Chile. Santiago, Expansiva. pp. 7-24. [en línea] <https://www.consejotransparencia.cl/category_estudios/publicaciones-cplt/> [consulta: 23 de diciembre de 2018]

BAELO, R. y Cantón, I. 2009. Las tecnologías de la información y la comunicación en la educación superior. Estudio descriptivo y de revisión. 2p. [en línea] <https://rieoei.org/historico/deloslectores/3034Baelo.pdf> [Consulta: 17 de marzo de 2020].

BARRIO, M. 2018. Internet de las cosas. Madrid. Editorial Reus. 128p.

BARROS, Enrique. 2010. Tratado de responsabilidad extracontractual. Santiago, Editorial Jurídica de Chile. 1.232p

CERDA, Alberto. 2003. Intimidad de los trabajadores y Tratamiento de datos personales por los empleadores. En: Revista Chilena de Derecho Informático(2): 35-59.

CERDA, A. 2012. Legislación sobre protección de las personas frente al tratamiento de datos personales. Santiago, Centro de Estudios de Derecho Informático de la Facultad de Derecho de la Universidad de Chile. 42p.

COMITÉ EVALUACIÓN DE LA LEY/OCDE. 2016. Evaluación de la Ley N° 19.628. 90p. En línea: <http://www.evaluaciondelaley.cl/informes-leyes-evaluadas/foro_ciudadano/2012-12-11/164002.html> [consulta: 25 de diciembre de 2018]

CORRAL, H. 2001. De los derechos de las personas sobre los responsables de bancos de datos: el hábeas data chileno. En: Cuadernos de Extensión Jurídica. Universidad de Los Andes(5): 39-59.

CORRAL, H. 2004. Lecciones de Responsabilidad Civil Extracontractual. Santiago, Editorial Jurídica de Chile. 423p.

DÁVARA, M. A. 1997. Manual de Derecho Informático. Madrid, Editorial Aranzadi. 396p.

FUNDACIÓN TELEFÓNICA. 2017. Economía de los Datos: Riqueza 4.0. Madrid, Editorial Ariel S.A. 180p.

GAJARDO, M. C. 2014. El Deber de Seguridad. En: Revista Chilena de Derecho del Trabajo y de la Seguridad Social 5(9): 15-32.

GARRIDO, R. 2015. La seguridad en el tratamiento de datos personales. En: Ciudadanas 2020 III: El gobierno de la información. Santiago, Instituto Chileno de Derecho y Tencología. pp. 77-92.

GARRIDO, R y BECKER, S. 2017. La biometría en Chile y sus riesgos. En: Revista Chilena de Derecho y Tecnología(6): 67-91.

GIMÉNEZ, V. 2011. Hacking y ciberdelito. Memoria para obtener el título de Ingeniero Técnico en Informática de Gestión. Valencia, Universidad Politécnica de Valencia. 123p. [en línea] <https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf> [consulta: 17 de marzo de 2020]

GOZAINI, O. 20010. Hábeas data. Protección de datos personales. Doctrina y jurisprudencia. Buenos Aires, Rubinzal-Culzoni. 526p.

GRIMALT, P. 1999. La responsabilidad civil en el tratamiento automatizado de datos personales. Granada, Editorial Comares. 382p.

HEREDERO, M. 1997. La Directiva Comunitaria de Protección de los Datos de Carácter Personal. Madrid, Editorial Aranzadi. 372p.

HERRÁN, A. 2002. El Derecho a la Intimidad en la nueva ley orgánica de protección de datos personales. Madrid, Dykinson. 388p.

HISTORIA DE LA LEY N°19.628. [en línea] <https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/6814/> [fecha de consulta: 21 de diciembre de 2018].

JERVIS, P. 2003. Derechos del titular de Datos y Habeas Data en la Ley 19.628. En: Revista Chilena de Derecho Informático(2): 19-33.

JERVIS, P. 2005. Categorías de datos reconocidas en la Ley 19.628. En: Revista Chilena de Derecho Informático(6): 111-145.

JERVIS, P. 2006. La regulación del mercado de datos personales en Chile. Tesis para optar al grado de Magíster en Derecho. Santiago, Universidad de Chile, Facultad de Derecho. 314p.

MARTÍNEZ, F. 1996. La enseñanza ante los nuevos canales de información. En: TEJEDOR, F. J. y GARCÍA, A.: Perspectivas de las nuevas tecnologías en la educación. Madrid. Narcea: 101-119.

MATÉ, C. 2014. Big data un nuevo paradigma de análisis de datos. [en línea] <https://www.iit.comillas.edu/docs/IIT-14-153A.pdf> [consulta: 17 de marzo 2020]

MURILLO DE LA CUEVA, P. 1990. El Derecho a la Autodeterminación Informativa. La Protección de los Datos Personales frente a la Informática. Madrid, Editorial Tecnos. 209p.

MURILLO DE LA CUEVA, P. 2008. El derecho a la autodeterminación informativa y la protección de datos personales. En: Azpilcueta: Cuadernos de Derecho (20): 43-58.

PARADA, B. 2008. El régimen de responsabilidad civil en la protección de datos personales en Chile. Memoria de Licencia en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile, Facultad de Derecho.

PÉREZ, A. 2017. Tutela sumaria de derechos en el proceso civil: misión y visión en Latinoamérica. En: Revista Chilena de Derecho Privado(28): 137-182.

RAJEVIC, E. 2011. Protección de datos y transparencia en la administración pública chilena: Inevitable y deseable ponderación. En: Reflexiones sobre el uso y abuso de los datos personales en Chile. Santiago, Expansiva. pp. 137-157. [en línea]

https://www.consejotransparencia.cl/category_estudios/publicaciones-cplt/ [fecha de consulta: 23 de diciembre de 2018]

RODRÍGUEZ, P. 2010. Responsabilidad Extracontractual. 2ª Edición. Santiago, Editorial Jurídica de Chile. 552p. [en línea] <http://app.vlex.com.uchile.idm.oclc.org/#CL/sources/6162> [consulta: 28 de diciembre de 2018]

ROSTIÓN, I. 2015. Sobre la Ley de Protección de la Vida Privada: La importancia de una "fuente legal" y su aplicación en las Personas Jurídicas. En: Revista Ius et Praxis 21(2): 499-520.

RUIZ, A. 1999. Los datos de carácter personal: concepto, requisitos de circulación, procedimientos, normativa y formularios. Barcelona, Bosch. 208p.

SUÑÉ, E. 2000. Tratado de Derecho Informático. Introducción y protección de datos personales. Madrid. Servicio de Publicaciones Universidad Complutense de Madrid. Vol.1.

VIOLLIER, P. 2017. El estado de la protección de datos personales en Chile. Santiago, ONG Derechos Digitales. 51p. [en línea] <https://www.derechosdigitales.org/tipo_publicacion/publicaciones/> [consulta: 12 enero 2019]

WARREN, S. y BRANDEIS, L. 1890. The Right to Privacy. En: Harvard Law Review 4(5): 193-220.

ZABALLOS, P. 2013. La protección de datos personales en España: evolución normativa y criterios de aplicación. Memoria para optar al grado de Doctor en Derecho. Madrid, Universidad Complutense de Madrid, Facultad de Derecho. 507p.

Legislación nacional

CÓDIGOS

Código Civil. 31 de mayo de 1856.

Código de Procedimiento Civil. 30 de agosto 1902.

Código del Trabajo. 16 de enero 2003.

LEYES

CHILE. Ministerio de Hacienda. 1997. Decreto con Fuerza de Ley 3: Fija texto refundido, sistematizado y concordado de la Ley General de Bancos y de otros cuerpos legales que se indican. 19 de diciembre 1997.

CHILE. Ministerio Secretaría General de la Presidencia. 1999. Ley 19.628: Sobre Protección de la Vida Privada. 28 de agosto 1999.

CHILE. Ministerio Secretaría General de la Presidencia. Ley 20.285: Sobre Acceso a la Información Pública. 20 de agosto 2008.

CHILE. Ministerio de Economía, Fomento y Turismo. Ley 20.575: Establece el principio de finalidad en el tratamiento de datos. 17 de febrero 2012.

CHILE. Ministerio Secretaría General de la Presidencia. 2018. Ley 21.096: Consagra el derecho a protección de los datos personales. 16 de junio 2018.

Legislación comparada e instrumentos internacionales

ARGENTINA. Ley 25.326: Ley de Protección de los Datos Personales. 02 de noviembre año 2000.

ESTADOS UNIDOS. California Civil Code. 21 de marzo 1872.

ESTADOS UNIDOS. Public Law 106-102: Gramm-Leach-Bliley Act. Publicada 12 de noviembre 1999.

ESTADOS UNIDOS. Public Law 104-191: Health Insurance Portability and Accountability Act. 21 de agosto 1996.

MÉXICO. Ley Federal de Protección de Datos Personales en Posesión de Particulares. 05 de julio 2010.

ORGANIZACIÓN DE NACIONES UNIDAS. Declaración Universal de Derechos Humanos. 10 de diciembre 1948.

UNIÓN EUROPEA. Reglamento 2016/679: Reglamento General de Protección de Datos. 14 de abril 2016.

Normativa sectorial

SUPERINTENDENCIA DE BANCOS E INSTITUCIONES FINANCIERAS. Última versión de 2018. Capítulo 1-13 de la Recopilación Actualizada de Normas. [en línea]

<https://www.sbif.cl/sbifweb/servlet/LeyNorma?indice=3.1.2&LNAN=1> [consulta: 04 de enero de 2019]

SUPERINTENDENCIA DE BANCOS E INSTITUCIONES FINANCIERAS. Última versión de 2018. Capítulo 20-8 de la Recopilación Actualizada de Normas. 3p. [en línea] <https://www.sbif.cl/sbifweb/servlet/LeyNorma?indice=3.1.2&LNAN=1> [consulta: 04 de enero de 2019].

Páginas web

IEUAN, J. 2018. Data protection in the United States: overview. [en línea] <https://uk.practicallaw.thomsonreuters.com/6-502-0467> [consulta: 24 de diciembre de 2018]

PULSO. 2019. Ciberseguridad: los desafíos de los reguladores para 2019. [en línea] La Tercera, suplemento Pulso. 05 de enero, 2019. <https://www.latercera.com/pulso/noticia/ciberseguridad-los-desafios-los-reguladores-2019/472866/#> [consulta: 11 de enero de 2019]