Universidad de Chile
Facultad de Derecho
Departamento de Derecho Comercial

LA FINALIDAD COMO ESTÁNDAR DE PROTECCIÓN DE DATOS PERSONALES DE CARÁCTER ECONÓMICO, FINANCIERO, BANCARIO Y COMERCIAL. UN ANÁLISIS DESDE LA EVOLUCIÓN NORMATIVA NACIONAL Y LA REGULACIÓN SUPRANACIONAL.

Memoria de prueba para optar al grado de Licenciado en Ciencias Jurídicas y Sociales

Ignacio Zegers Uauy

Profesor guía: Claudio Paul Magliona Markovitcth

Santiago, 2021

Dedicada a mi familia, especialmente a la Coya. También a la Biblioteca.

Resumen

En este texto se realizará un análisis acerca de una particular manifestación que tiene el derecho fundamental de la privacidad, los datos personales. Concretamente hablando, se expondrá sobre los datos personales de carácter económico, financiero, bancario y comercial, los cuales son de absoluta importancia en el desempeño del comercio electrónico. Además, se expondrá sobre como la normativa en Chile durante las últimas décadas ha abordado esta materia desde la perspectiva de un principio rector en el tema: el principio de finalidad. A este respecto, como se verá más adelante, las normas vigentes ante este fenómeno son insuficientes para poder realizar una protección adecuada de los datos personales de carácter pecuniario de los particulares. Ante este escenario, se hará una exposición y análisis sobre como en el panorama internacional se regula esta materia desde principalmente una perspectiva supranacional y de cómo se utiliza el principio de finalidad para tratar estos temas. Finalmente, se abordará y analizará de manera crítica los desafíos que existen hoy en día para nuestro país, y de cómo este tema se ha debatido de cara al proyecto de ley que busca cambiar estructuralmente el régimen de la protección de la privacidad en Chile.

Palabras clave: finalidad, protección de datos, derecho a la privacidad, estándares de protección, avances tecnológicos.

Abstract

This text will develop an analysis about a particular manifestation that the fundamental right to privacy has, personal data. Concretely speaking, we will discuss personal data of economic, financial, banking and commercial nature, which are of absolute importance in the performance of electronic commerce. Furthermore, we will discuss how the legislation in Chile during the last decades has approached the matter from the perspective of the governing principle of the topic: the principle of finality. This regarding, as it shall be seen later on, the current norms in the face of this phenomenon are insufficient to be able to realize an adequate protection of the personal data of pecuniary nature of the individuals. In view of this scenario, we will make an exhibition and an analysis about how in the international outlook this subject is regulated mainly from a supranational perspective and how it is utilized the principle of finality to process these topics. Finally, we will approach and analyze in a critical manner the challenges that exist today for our country, and how this topic has been debated regarding the bill that searches to structurally change the regime of privacy protection in Chile.

Keywords: purpose, data protection, right to privacy, protection standards, technological advances.

TABLA DE CONTENIDO

INTRODUCCIÓN

La necesidad de investigar acerca de cómo interactúa la protección de datos personales con el derecho nace de una premisa extremadamente simple: el mundo en el que vivimos es cada vez más interconectado en términos informáticos. Durante el último tiempo, y en especial dadas las complejas circunstancias sanitarias que se han vivido en todo el planeta, la interconectividad pasó de ser un simple hecho conocido por todas las personas, a ser prácticamente lo que configura toda nuestra realidad como sociedad. La verdad de las cosas es que la sociedad de la información nunca se había manifestado con tanta intensidad como en la actualidad lo está haciendo, pues la red y las plataformas han pasado de ser de una herramienta útil para realizar ciertas actividades, al medio por el cual hacemos toda nuestra vida, incluso nuestras interacciones interpersonales.

En este contexto, es que los datos personales como materia de estudio ya no solo es una discusión acerca de cómo hacer valer en determinadas situaciones la protección de la intimidad y privacidad de las personas y de sus demás derechos fundamentales. La discusión de esta materia ha devenido en la cuestión de cómo poder vivir resguardando nuestra personalidad y toda nuestra privacidad en esta nueva sociedad informática, que ya ha definitivamente emergido de la mano de los agigantados avances tecnológicos y que cada día sigue avanzando con más fuerza que el anterior. La máxima manifestación de todo esto es el fenómeno del Big Data, el cual se puede ilustrar de manera muy clara con la siguiente definición:

> *"…en términos generales podríamos referirnos como a la tendencia en el avance de la tecnología que ha abierto las puertas hacia un nuevo enfoque de entendimiento y toma de decisiones, la cual es utilizada para describir enormes cantidades de datos (estructurados, no estructurados y semi estructurados) que tomaría demasiado tiempo y sería muy costoso cargarlos a un base de datos relacional para su análisis. De tal manera que, el concepto de Big Data aplica para toda aquella información que no puede ser procesada o analizada utilizando procesos o herramientas tradicionales."*[1]

No está de más mencionar que esta realidad deviene en un gran desafío para la democracia, las instituciones y todos los diversos ámbitos que conllevan la vida en sociedad,

[1] BARRANCO, R. (2012) "¿Qué es el Big Data?" IBM Developer Works. [en línea] Disponible en: https://developer.ibm.com/es/articles/que-es-big-data/ [consultado el 8/12/21]

pues se ha llegado a un punto en que el tratamiento de datos ya no se hace solo de manera consciente, sino que ocurre en esta vida digital que existe circulación y tratamiento de aquellos datos que el titular genera con cada movimiento que realiza en línea (metadata) y que por lo general desconoce y se encuentra más allá de su control.[2]

Este panorama afecta toda clase de información personal o sensible que tanto las personas naturales como las jurídicas poseen, y en este entendido nuestros datos económicos y financieros no son la excepción. La utilización de plataformas y documentos físicos o digitales que contienen esta clase de información tienen hoy por hoy importantes consecuencias en cómo se desempeña actualmente la economía. Este fenómeno se ve manifestado en la realidad de un ya hegemónico comercio electrónico, que implica necesariamente el uso de datos personales con contenido pecuniario de los usuarios y consumidores para su funcionamiento. A su vez, se expresa en plataformas en donde se amacena información referente a las deudas impagas de consumidores, como puede ser por ejemplo DICOM. Es justamente en esa línea que se necesita encontrar un equilibrio para poder ponderar adecuadamente el interés de que el intercambio de servicios y bienes se dé en los mercados digitales de manera fluida con el de resguardar la integridad de los derechos de los usuarios de estos mismos. La tensión de estos intereses que a veces pueden llegar a ser incluso contrapuestos es uno de los asuntos que se intentará abordar en este texto, particularmente se estudiará el tema desde la perspectiva de uno de los principios rectores de la protección de la privacidad: el principio de finalidad. Como se verá, este principio es troncal en el ámbito de la protección de datos personales, y en ese sentido permea la regulación de los datos personales y su tratamiento en todas sus facetas, y tiene características particulares en el ámbito de su aplicación a los datos que tienen relevancia en el contexto del mundo económico y financiero.

De este modo, a lo largo de esta monografía se van a tocar y analizar una serie de temas que son de interés para el estudio de la temática propuesta. Es así como en primer lugar se identificará cómo ha evolucionado el régimen la protección y de la privacidad que se encuentra en nuestro país llegando a la normativa actual, si bien en un principio se hará una breve reseña sobre el Derecho Fundamental de la privacidad y del régimen general de su protección, terminaremos enfocándonos particularmente en la información personal económica y financiera de las personas. Una vez diagnosticado todo este panorama, se hará

[2] MILANES, V. (2017). “Desafíos en el debate de la protección de datos para Latinoamérica” Transparencia & Sociedad, No. 5, p. 13

un análisis crítico de, por un lado, cómo ha evolucionado esta materia en el ámbito internacional (particularmente desde la perspectiva supranacional) durante los últimos años, y por otro, del último proyecto de ley que se ha presentado en nuestro país en esta materia. Con toda esta información, se podrán obtener una serie de conclusiones de cómo toda esta evolución normativa intenta acercarse a un régimen que permita este equilibrio que hemos expuesto en donde se pueda ponderar adecuadamente las transacciones comerciales electrónicas y los derechos fundamentales de los usuarios, además de los respectivos desafíos que la actualidad se presentan en este ámbito y de cómo estos deben enfrentarse para poder hablar en el futuro al interior de nuestro país de un régimen de protección de la privacidad que dé cuenta de los avances tecnológicos del siglo XXI.

CAPÍTULO 1: El régimen de protección de los datos personales en Chile.

I. El derecho fundamental de la privacidad

El punto de partida necesario para desarrollar el tema propuesto es sin duda la privacidad como derecho fundamental. En la tradición continental y chilena, este derecho significa básicamente que cierta información de las personas es secreta, aunque en Chile particularmente también se ha reconocido por la doctrina que este derecho incluye una noción de autonomía, además de que cierta jurisprudencia ha reconocido la privacidad como manifestación de la tranquilidad.[3] En términos generales desde el panorama internacional, la Declaración Universal de los Derechos Humanos, se recoge este derecho en su artículo 12, que dispone que 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. El artículo añade que toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. De este modo, se puede afirmar que existe una obligación de origen internacional de respetar este derecho, siendo los sujetos obligados los Estados. Esto guarda total coherencia con el que en Chile se considere la privacidad como un Derecho Fundamental.

En términos de nuestra normativa nacional, este derecho se encuentra consagrado constitucionalmente en los numerales 4 y 5 del artículo 19 de nuestra Constitución Política de la República (CPR), en donde se dispone que la Constitución asegura a todas las personas en primer lugar *"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."* Agrega este numeral que *"el tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley".* Y, en segundo lugar: *"La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley".* Es relevante mencionar que, si bien la privacidad en términos generales es tratada por el texto constitucional en dos numerales separados, la doctrina entiende de forma prácticamente unánime que el numeral quinto del artículo 19 es una especificación de lo dispuesto en el numeral cuarto, no un derecho distinto.[4] Respecto del numeral cuarto del artículo 19, también cabe recalcar que su actual

[3] FIGUEROA, R. (2020) Derecho de privacidad. En: Curso de Derechos Fundamentales. Editorial Tirant lo Blanch. p. 129
[4] *Ibid.* p. 132

redacción no es la que originalmente poseía el texto de nuestra carta fundamental cuando esta entró en vigencia. Durante el año 2018, se hace una reforma constitucional por medio de la ley N° 21.096, con la cual se agrega todo lo relacionado con la protección de datos que este apartado dispone. Como se puede notar de la historia fidedigna de esta Ley, la moción de impulsar el reconocimiento en la carta magna chilena de la protección de datos responde a las severas críticas que la regulación de esta materia, y a un intento de adecuarse a los estándares internacionales.[5] Como veremos, el resguardo y protección de la privacidad ha sido un tema de alta complejidad al interior de nuestro ordenamiento jurídico, que se ha visto muy dejado de lado durante los últimos años, y su regulación legal vigente ha sido objeto de diversas críticas por parte de la academia y de las diferentes organizaciones civiles al interior de la sociedad.

Finalmente, a propósito de su regulación constitucional, cabe mencionar que este derecho se puede ver tutelado por medio de la acción de protección, según lo dispuesto en el artículo 20 CPR. Esta última observación es relevante, para efectos de entender cómo se ha dado la protección de la privacidad en nuestro país, y particularmente respecto de cómo se dio con anterioridad a la entrada en vigencia de la Ley de Protección de la Vida Privada (ley N° 19.628) durante el año 1999.

Ahora bien, resulta muy importante para el análisis que se hará posteriormente indicar que, desde la óptica de la sociedad postindustrial, el derecho de la privacidad no solo ha concebido como una libertad negativa, sino también una positiva; puesto que, se trata no solo de tutelar la subjetividad de la injerencia ajena (estatal o privada), sino de preservar la identidad y libertad frente al intenso e invisible poder informático.[6] Esto hay que tenerlo en especial consideración con la realidad actual, donde el caudal de información personal de los individuos y las personas jurídicas es susceptible de ser tratado por medios informáticos y aún transmitida a distancia gracias al desarrollo de las telecomunicaciones y a la red digital, manifestada en el Internet. Esta aptitud tecnológica tiene su manifestación más radical en el procesamiento automático de datos y el fenómeno del Big Data ya mencionado previamente. Todo esto ha despertado la precaución de quienes creen ver en ello un serio riesgo para los derechos fundamentales, desde que permite a quien dispone de la información acceder a aspectos de

[5] CHILE, Congreso nacional de Chile. Primer trámite en Comisión de Constitución del Senado, que recae en la moción parlamentaria para reforma constitucional que consagra el derecho a la protección de los datos personales. Boletín N° 9.384-07. 2014. p.3

[6] ZÚÑIGA, Francisco. (2000), "Criterios para la conciliación entre la libertad de información y el derecho a la vida privada en la jurisprudencia internacional y nacional", en: *Revista "Ius et Praxis", Facultad de Ciencias Jurídicas y Sociales, Universidad de Talca, Año 6 N.º 1 Editorial Universidad de Talca,* Talca, Chile. p. 288.,

nuestra vida que legítimamente deben ser resguardados, y aún servirse de ella para condicionar el ejercicio de nuestras libertades."[7]

Ante este escenario, es que se ha desarrollado desde una perspectiva doctrinaria el así llamado derecho de autodeterminación informática, el cual si bien ha quedado sujeto a una intensa discusión si es un derecho autónomo, distinto al derecho a la privacidad o no, ante todo, hace referencia a la protección de todo dato que se predica en una persona, de cómo esta los administra, y de cómo terceros pueden hacer uso de tales datos. [8] Por otro lado, se ha indicado que, como ya se adelantó más arriba, este derecho junto al derecho a la honra se encuentra indisolublemente vinculado con el reconocimiento de la personalidad y de la autonomía de los individuos que integran a la sociedad. Así, la honra y la privacidad son bienes fundados sin mayor dificultad en la dignidad de la persona, porque exigen respetar su pretensión de validación social, así como en el derecho a desarrollar libremente su personalidad, porque reconocen un espacio privado de acción que sólo al titular corresponde abrir hacia terceros.[9] Como un adelanto a lo que se verá más adelante, a juicio de cierta doctrina, el principio de finalidad es un elemento central en la idea del derecho de autodeterminación informativa, ya que este garantiza a los ciudadanos la posibilidad de controlar el uso de sus datos personales, ofreciéndole una respuesta precisa y concreta a la cuestión de para qué van a ser utilizados, impidiendo además usos diferentes o incompatibles.

De este modo, podemos ver como la privacidad es un derecho fundamental arraigado a la autonomía de las personas y su correlativa autodeterminación y desenvolvimiento en el mundo. Es por todo esto que se fundamenta la necesidad de resguardar la información e intimidad, la cual se busca proteger ante la injerencia de terceros, ya sean estos entes públicos o privados. Como se verá en su momento, el paradigma del consentimiento es muy relevante en este aspecto, especialmente respecto del tratamiento de datos personales. Cabe mencionar que es posible atentar contra la privacidad de más de una manera. Una de las alternativas posibles es adquiriendo información personal contra el consentimiento de quien la detenta, otra posibilidad de que esto ocurra es traicionando los fines para los cuales el particular prestó su consentimiento al usar tal información para fines diversos. Respecto de este segundo modo de afectar la privacidad ahondaremos en esta monografía, ya que la

[7] CERDA, Alberto.(2012), "Legislación sobre protección de las personas frente al tratamiento de datos personales". *Apuntes de clases, Centro de Estudios en Derecho Informático, Universidad de Chile.* p.8

[8] GARRIGA, A. (2016)," Nuevos retos para la protección de los datos personales en la era del Big Data y de la computación ubicua" Editorial Dykinson, España. p.97

[9] BARROS, Enrique. (2010), Tratado de Responsabilidad Extracontractual. Santiago, Chile. Editorial Jurídica de Chile, p. 536

desviación de los fines se encuentra arraigado hasta sus cimientos más profundos con el principio de la finalidad en los datos personales.

Hecho este análisis, corresponde ahora ahondar en cuál es el contenido del derecho a la privacidad, es decir, qué es lo que se protege exactamente al tutelar este derecho. Al respecto, se puede apreciar que son muchas las cosas que quedan protegidas por este derecho, como por ejemplo los paradigmas más propios de nuestra intimidad, como la vida sexual o las convicciones ideológicas, o bien, objetos o documentos que son de tal importancia e interés para determinados individuos, que no deben ser expuestos al público sin el consentimiento expreso del titular, como pude ser la ficha medica de un paciente o la información financiera de una persona en particular. Estos documentos, cuyo contenido es de alto interés para una persona (que puede ser natural o jurídica por supuesto), y que naturalmente pueden encontrarse en formato digital, son los que se entienden que se constituyen como "datos personales".

En este texto nos vamos a enfocar en aquellos documentos, especialmente digitales, de carácter económico que revisten la característica de ser datos personales de una persona, los cuales pueden usarse con el permiso (o bien, en términos de nuestra Ley de Protección de la Vida Privada como veremos, sin este permiso) del usuario para determinados fines, esto en especial en el contexto del comercio electrónico, de las bases de datos que contienen información respecto de la solvencia de una persona, entre otros fenómenos y plataformas. Para finalizar esta sección, cabe mencionar que la protección de la privacidad referente a objetos es una materia que no ha sido estudiada de manera sistemática en la doctrina nacional, aun cuando en el artículo 19 N° 5 de la Constitución Política vigente se hace referencia explícita a la protección de las comunicaciones y los documentos privados.[10]

II. La ley N° 19.628

Lo primero que merece ser comentado sobre este cuerpo normativo, conocido como "Ley Sobre Protección de la Vida Privada", es que durante su tramitación, se determinó en la cámara de diputados que esta Ley, que tenía por objeto original regular la protección en general de la vida privada, pasaría a ser una ley específica y dedicada a los datos personales, que respondiera a ciertos principios como la legitimidad de los medios para la recolección de

[10] FIGUEROA, R (2020). *Op. Cit.* p. 139

datos personales, la finalidad como factor determinante de la licitud del tratamiento y el resguardo de antecedentes que constituyen "información sensible".[11]

Durante mucho tiempo, la ya mencionada anteriormente acción constitucional de protección contenida en el artículo 20 de la Constitución Política fue el único medio procesal para obtener tutela ante los tribunales de justicia, cuando había un tratamiento indebido de datos personales y en la medida que, en algún sentido, se vulnerara o perturbara el ejercicio del derecho a la vida privada o la honra de los afectados.[12] En este panorama, cabe mencionar que al no existir durante aquella época una consagración de rango constitucional expresa de la protección de datos personales, ni tampoco una consagración normativa del ya mencionado derecho a la autodeterminación informativa, fue este el medio procesal que tanto la doctrina como la jurisprudencia interpretaron como el más idóneo acorde al derecho vigente para tutelar de cierto modo este derecho.

Con la promulgación de la ley N°19.628 durante el mes de agosto del año 1999, por primera vez en nuestro país se tiene a nivel legal una normativa que se ocupe directamente de la tutela y protección de datos personales. Como se aprecia en la historia de la ley, el objetivo que se tenía con esta legislación era "llenar un vacío manifiesto en nuestro ordenamiento jurídico y cuyo propósito es dar una adecuada protección al derecho a la privacidad de las personas, en el ámbito del Derecho Civil, ante eventuales intromisiones ilegítimas".[13] De este modo, Chile se suma a los países que comienza a tener legislación positivizada de esta materia, siendo por lo demás pionero en la época respecto de ciertos aspectos de esta regulación, como por ejemplo la exigencia contenida en su cuarto artículo, en referencia al consentimiento del titular, el cual como se verá, debe ser según ley expreso y escrito.[14]

Lo primero que se puede consignar al respecto de esta ley, es que, esta entiende por dato personal en su artículo 2 letra f) *"aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables*". En este entendido, siendo su principal objetivo como hemos visto el otorgar protección a este tipo de información en particular, establece en la letra o) de la norma recién citada una definición de tratamiento de datos,

[11] La privacidad en el sistema legal chileno. (2014) Por Carolina Pincheira "et al". ONG Derechos Digitales. p. 29
[12] VIOLLIER, P. (2017), "El estado de la protección de datos personales en Chile", ONG derechos digitales Latinoamérica p.7
[13] CHILE, Congreso Nacional de Chile. Primer trámite de Constitución en el Senado de la Ley N°19.628 sobre datos personales.1999. p.3
[14] BAUZÁ, F. (2019). El modelo europeo de protección de datos. Experiencias para la regulación chilena presente y futura*. Ars Boni et Aequi, Año N° 15, N° 1,* p. 128

entendiéndose como tal *"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."* A partir de las definiciones citadas, es que se puede ver a grandes rasgos las consideraciones generales que se buscaban proteger referentes a los datos personales.

En esta línea, la ley en su artículo cuarto dispone que el tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello. En ese apartado, ya podemos ver cómo se pone énfasis en la autonomía de la persona como fundamento de su privacidad, al indicar que el uso de datos personales solo se encontrará autorizado por la legislación o por el consentimiento expreso de la persona, dejando entonces, aparentemente, la autodeterminación de la persona como parámetro fundamental del uso de su información personal. Esta última idea, en el ámbito de los datos personales de carácter pecuniario es dudosa, por lo que veremos oportunamente.

III. El derecho de privacidad y datos de carácter financiero, económico, bancario y comercial.

Cuando nos referimos a esta clase de información, lo primero que debemos hacer es consignar que, como ya se ha mencionado, los datos de carácter pecuniario son un pilar fundamental para el funcionamiento de la economía digital. Esta aseveración no solo implica un fluido y eficiente tráfico de bienes y servicios por medio de plataformas digitales, sino que también, en la medida de que la regulación esté bien lograda, poder otorgar protección al consumidor en orden de impedir el mal uso de su información en ciertas situaciones, tales como el sobreendeudamiento y la insolvencia. En este sentido se ha dicho por ejemplo que los denominados sistemas de información crediticia (SIC) pueden ayudar a mejorar esta protección. Se entienden por SIC, el conjunto de bases de datos que suministran información acerca de la solvencia de personas físicas y jurídicas.[15]

[15] BOZZO, S. (2020). "Sobreendeudamiento, sistemas de información crediticia y la protección de los datos personales el consumidor en Chile" *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, segundo semestre del 2020.* P 102.

La relevancia de tratar estos datos de manera separada tiene dos fundamentos, uno de carácter cuantitativo, en atención a la cantidad de datos de clientes manejados por instituciones financieras, y un fundamento legal, referente a la insuficiencia regulatoria en lo que respecta a este tipo de información.[16]

La regulación de los datos de carácter financiero y económico en Chile se da por medio de varios cuerpos normativos. La primera expresión legislativa cuyo contenido buscaba hacerse cargo de esta materia que podemos identificar es el Decreto Supremo N° 950 del Ministerio de Hacienda del año 1928. En su primer artículo, se enumeran una serie de datos que todas las oficinas de la república deberán comunicar a la Cámara de Comercio de Chile en Santiago. Entre la información que el artículo enlista, podemos encontrar: lista de compraventas, mutuos hipotecarios, convenios extrajudiciales con comerciantes, etc. Por su parte, el artículo 3 de este decreto establece que es responsabilidad de la Cámara de Comercio de Santiago el publicar bajo su vigilancia un boletín semanal que contenga los datos señalados en el primer artículo. Así, estas publicaciones se constituyen como el primer tráfico y tratamiento de datos financieros que se da regulado de manera normativa en nuestro país.

Otro cuerpo normativo que evidentemente es relevante en este ámbito protección es la Ley N° 19.628. En este entendido, uno de los primeros puntos en donde se hace una referencia explícita a los datos que revisten esta característica es en el tercer inciso de su artículo 9. La norma dispone que se prohíbe la realización de todo tipo de predicciones o evaluaciones de riesgo comercial que no estén basadas únicamente en información objetiva relativa a las morosidades o protestos de las personas naturales o jurídicas de las cuales se informan. Así, podemos ver como la norma tiene un enfoque en la fuente de la información financiera que se divulga, con el objeto de poder asegurar que esta esté basada en parámetros objetivos, y que por lo tanto sea fidedigna. El mismo inciso dispone que la infracción a esta prohibición obligará a la eliminación inmediata de dicha información por parte del responsable de la base de datos y dará lugar a la indemnización de perjuicios que corresponda.

Continuando con el estudio de la ley 19.628, podemos notar que la matriz de la protección de la información pecuniaria se extrae a partir de lo dispuesto a partir del título III de la Ley, en el cual se dispone todo lo relacionado con la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial. El art 17 de la Ley, que es el primero del título en análisis, establece el marco por el cual los responsables

[16] La privacidad en el sistema legal chileno. (2014) *Op. Cit.* p. 90

de los registros y bancos de datos sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, en determinadas circunstancias contempladas por ley (que consten en pagares, letras de cambio protestados, cheques también protestados, entre otros). Es relevante mencionar además que el segundo inciso de la norma en análisis establece que también podrán comunicarse aquellas otras obligaciones de dinero que determine el Presidente de la República mediante Decreto Supremo, las que deberán estar sustentadas en instrumentos de pago o de crédito válidamente emitidos, en los cuales conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento. Como se puede ver, la norma establece determinadas causales expresas respecto de la cual entidades que administran la información financiera de los particulares pueden ser comunicadas a otras personas. Así las cosas, la ley dispone en su artículo 18 que en ningún caso pueden comunicarse los datos que se relacionen con otra persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible. Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de haber sido pagada o haberse extinguido de modo legal. Ante todo, se comunicarán a los tribunales aquella información que requieran en el contexto de juicios pendientes. De este modo, estos dos artículos muestran los parámetros generales respecto de los cuales se puede manipular la información financiera de una determinada persona por parte de un banco de datos u alguna otra entidad que administre tales registros.

Dicho todo lo anterior, y sin perjuicio de que la temática que se expondrá en este párrafo será analizada con más detención en la siguiente sección de este capítulo, es de suma importancia adelantar de que uno de los puntos más discutibles que tiene la ley N° 19.628 es justamente referente a los datos financieros, pues tal como se indica en el art. 4, no se requerirá del consentimiento del titular para el tratamiento y tráfico de datos de carácter económico, financiero, bancario o comercial. Esta norma es de extrema sensibilidad a la luz de los derechos de las personas y puede resultar muy lesiva. Como ya se dijo, las implicancias de esta norma, sus respectivas críticas y como ha actuado el legislador ante los problemas que esto presenta se revisará con mayor detención con posteridad en este texto.

Para finalizar con esta visión general a la regulación de la información económica, resulta muy relevante a su vez la Ley General de Bancos, la cual también toca esta materia al interior de su articulado. Esta ley, hace una distinción entre información sujeta a secreto y la información reservada[17]. Respecto del primer tipo de información, es decir, aquella sujeta a

[17] *Ibid.* p.91

secreto, es relevante lo dispuesto en el artículo 149, referente a las operaciones de depósitos y captaciones, las cuales, en virtud de esta norma, se encuentran sujetas a secreto bancario y por lo tanto no podrán proporcionarse antecedentes relativos a dichas operaciones sino a su titular o a quien haya sido expresamente autorizado por él o a la persona que lo represente legalmente. Quien contravenga esto, según lo dispuesto en la misma norma, puede arriesgar la pena de reclusión menor en sus grados mínimo a medio. Por su parte, el segundo inciso de la norma nos indica la información sujeta a reserva, las cuales se constituyen como aquella referente a cualquier otra operación que no sea de depósito y captación. Ahora, respecto del segundo tipo de información, es decir, la información reservada, podemos decir que tiene como característica fundamental que los bancos en virtud de la presente ley solamente podrán darla a conocer a quien demuestre un interés legítimo y siempre que no sea previsible que el conocimiento de los antecedentes pueda ocasionar un daño patrimonial al cliente. De este modo, podemos ver cómo esta ley agrega un parámetro extra de protección de la financiera de los usuarios, al declarar determinada información como secreta con el propósito de poder resguardar a los clientes,(llegando al punto de poner sanciones de carácter penal en caso de pasar a llevar tal información) como de poner requisitos determinados para información reservada, de modo de que terceros no puedan ocasionar un daño patrimonial con esos datos al titular.

IV. Críticas a la ley de protección de la vida privada

Dicho todo lo anterior, esta ley ha sido objeto de intensas controversias y críticas, las cuales comenzaron incluso durante la época de su tramitación, y que se intensificaron desde el momento en que fue promulgada en el diario oficial. Ante todo, estas críticas han apuntado a que se trata de una ley que resulta insuficiente para poder hacer una correcta protección del derecho a la intimidad de las personas y de sus datos personales ante la injerencia de terceros.[18] Los problemas que vienen aparejados en este sentido, se pueden ver en dos categorías. En primer lugar, problemas que son propios de cómo es la redacción de lo dispuesto en la ley, que lleva a incertezas de su interpretación y aplicación, y, en segundo lugar, problemáticas asociadas a la estructura legal y administrativa por medio de la cual los derechos consagrados en la ley se hacen valer.

[18] VIOLLIER, P. (2017), Op. Cit. p.7, 8

Dentro de la primera clase de problemas, podemos identificar que la ley no establece al interior de su articulado una definición expresa de consentimiento (cosa que cuerpos normativos en el extranjero que son contemporáneos a la época ya lo hacían, como por ejemplo la Directiva 95/46/CE de la Unión Europea, la cual será analizada en su momento). Esta situación deja una base excesivamente amplia de interpretación acerca de esta temática. Esta es una situación muy sensible al ser el consentimiento un elemento de gran relevancia en cuanto a la protección de los datos personales desde la perspectiva de la finalidad y de la regulación de este asunto en general. Esto es muy relevante, además, porque tal como se estructura la ley, esta establece una serie de excepciones respecto a ciertas situaciones en las cuales no se requerirá del consentimiento para efectos del tratamiento. Estas situaciones se encuentran en el artículo 4 inciso quinto de la ley en análisis, a saber:

1) datos personales que provengan o que se recolecten de fuentes accesibles al público,

2) cuando sean de carácter económico, financiero, bancario o comercial,

3) se contengan en listados relativos a una categoría de personas que se limiten a indicar determinados antecedentes, o

4) sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Este inciso ha sido duramente criticado, pues se ha apreciado que del contexto de las normas se desprende que la mayoría de los datos provienen de "fuentes de acceso público" y se consagran importantes y amplias excepciones sobre todo en materia de datos "personales-patrimoniales", lo cual transforma a la regla general en una mera declaración de principios.[19]

En este mismo entendido, resulta del todo criticable una de las causales de este inciso en particular, la excepción referente a que no se requerirá de tal autorización en caso de que el dato provenga de fuentes accesibles al público. Este supuesto ha generado controversia a nivel doctrinario respecto a su alcance[20]. Esto en el entendido de que la ley no especifica de manera suficiente el a qué se refiere con "fuente de acceso público", si vemos el artículo 2 letra i) de la Ley N° 19.628, este dispone que se entiende por fuente de acceso al público *"como los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes."* Esta definición, siendo muy ambigua, genera una

[19] Véase. JIJENA, R. (2001) "Sobre la no protección de la intimidad en Chile. Análisis de la Ley 19.628, de Agosto de 1999". *Revista Electrónica de Derecho Informático, N°39*. pp. 22- 24

[20] ALVARADO, F. (2014), "Las fuentes de acceso público a datos personales" *Revista Chilena de derecho y tecnología, N°3*.pp. 216-219

incerteza muy riesgosa, al ser una excepción con contornos difusos que se da en un contexto en que, si no se requiere consentimiento, la discrecionalidad del ente que realiza el tratamiento de datos aumenta de manera sustancial, lo cual puede resultar ser un riesgo para los derechos del titular. Una excepción de esta naturaleza entonces necesariamente debe tener límites definidos que logren generar certeza y así poder mitigar la mayor cantidad de riesgo posible, además de darle contorno al ámbito de control y acción del titular respecto de su información.

Finalmente, cabe mencionar que se ha criticado a su vez de manera particular la causal referente a aquella información que sea necesaria para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios. Esta excepción, se traduce inmediatamente a que el legislador autoriza expresamente que la entidad que realiza el tratamiento pueda utilizar esa información para efectos de marketing directo sin necesidad de ninguna autorización del titular. No es necesario entrar en un análisis exhaustivo para explicar el por qué una norma de esta naturaleza puede vulnerar el derecho a la privacidad del titular, además de potencialmente no solo irrogar un daño a la imagen de su persona, sino también a su integridad física y psicológica.

Como ya adelantamos, podemos identificar en segundo lugar problemas de carácter estructural, que impiden que se pueda efectuar una protección eficaz de los derechos informáticos de las personas. Entre los principales problemas que se han identificado que explican la insuficiencia de esta ley, está la falta de aspectos orgánicos esenciales, como por ejemplo la existencia de un registro de bases de datos particulares, de un ente fiscalizador, de un procedimiento de reclamo administrativo y de sanciones eficaces.[21] Estas fallas orgánicas por supuesto que se vuelven más sensibles en la medida en que nos adentramos en el siglo XXI y las comunicaciones comienzan un agresivo y rápido proceso de digitalización. Esto hace que tanto el almacenamiento como tráfico de datos en este formato no físico hagan que la protección se haga aún más necesaria. Si no se constata un diseño institucional capaz de poder responder ante estas consideraciones, los principios descritos más arriba en la ley quedan sin hacerse valer de manera adecuada y por lo tanto como una mera declaración de buenas intenciones. Es necesario que ante la posibilidad de que quien manipule la información de una persona en particular y se aleje de la finalidad para la cual se le entregó tal información, esta última entidad pague las consecuencias de haber incumplido lo acordado, y eso no se puede lograr sin una estructura que logre hacer valer tal responsabilidad de manera adecuada.

[21] JIJENA, R. (2010) “Actualidad de la protección de datos personales en América latina. El caso de Chile”, Memoria del XIV Congreso Iberoamericano de Derecho e Informática (Monterrey, UANL), p. 414

CAPÍTULO 2: El principio de finalidad

I. La lógica y fundamentos de los principios

Para adentrarnos de lleno en el principio de finalidad, lo primero que corresponde hacer es delimitar el concepto que será objeto de estudio en este capítulo para poder analizar los desafíos que presenta su implementación en el mundo real. Por principio, entendemos un conjunto de estándares que apuntan a decisiones particulares referentes a una obligación jurídica en determinadas circunstancias.[22] En este entendido, la particularidad que tienen los principios es que ordenan la voluntad y el comportamiento de los individuos de una manera genérica. Es en definitiva una directriz de la acción de determinadas personas e individuos que logran posibilitar la vida en comunidad al interior de la sociedad. Es importante recalcar que, desde esta concepción de los principios, estos son estándares que son diferentes a las normas, pues estos se constituyen como un conjunto de conceptos generales que obedecen a consideraciones de diversa naturaleza, tal como la equidad, la justicia, o las múltiples dimensiones de la moralidad,[23]mientras que las normas orientan el comportamiento de manera concreta a partir de un texto delimitado y positivizado. De este modo, un claro ejemplo de un principio general que podemos recoger respecto de la materia que este texto convoca, es que nadie puede pasar a llevar la privacidad de otro sin ningún fundamento que lo legitime, mientras que una norma puede ser la prohibición expresa de utilizar información específica de una persona sin su consentimiento, aparejada a una sanción determinada.

En este contexto, los principios son parte fundamental del derecho en todas sus facetas, y el derecho informático con todos sus pormenores correspondientes no es la excepción. La necesidad de salvaguardar los derechos fundamentales de las personas y poder tutelarlos cuando las circunstancias lo ameriten, implica el poder realizar un fiel seguimiento de un conjunto de principios que den cuenta de las normas jurídicas positivizadas y que en definitiva le dé sentido a la regulación de la materia que se trate. En relación con la protección de datos personales, existen varios principios que apuntan a esto, entre los cuales uno de los más importantes es justamente el principio de finalidad.

[22] DWORKIN. R. (1984) “Los Derechos en Serio” Editorial Ariel S.A. Barcelona, España. p. 75
[23] *Ibid.* p 72

II. La noción de finalidad en la ley 19.628

Con el propósito de ahondar en el objeto al que este texto busca hacerse cargo, corresponde analizar el principio de finalidad propiamente tal al interior de la Ley sobre protección de la vida privada. Como ya se adelantó, el legislador desde un inicio que se comenzó a discutir sobre esta materia tenía en mente una noción de la idea de finalidad como uno de los conceptos fundamentales para la protección de datos personales. Esto se puede ver en el ya citado artículo 1 inciso 2 de la ley N° 19.628, cuando se 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. Si bien cómo podemos ver es innegable que en la norma en análisis el legislador da luces de una noción de cuáles deben ser los fines que se deben perseguir con el uso de los datos, la norma citada es demasiado amplia para poder hablar del principio de finalidad de una manera concreta, pues los fines de la legislación y del ordenamiento jurídico son conceptos demasiado difusos que por lo demás pueden ser diversos a los del titular de los datos, además de que esta finalidad que se recoge en la norma en análisis no denota un contenido los suficientemente nítido como para saber en qué términos tal finalidad debe ser perseguida. Es por todo esto que ahora entraremos de lleno en cuál es la fisionomía de la finalidad en la privacidad y particularmente en los derechos digitales.

Este principio, como se ha indicado desde la doctrina, ordena que los datos personales solo pueden utilizarse y tratarse para los fines por los cuales fueron recolectados. Este principio se encuentra estrechamente relacionado con otro ,más amplio, el principio de información y consentimiento del titular, ya que resultaría ilegítimo que los datos fueran utilizados para fines distintos que los consentidos por quien es titular de estos mismos.[24] De este modo, podemos ver que el principio de finalidad no solo hace referencia a “los fines permitidos por el ordenamiento jurídico” como lo indica el artículo primero de la ley de datos personales ya comentado, sino que a los fines que el propio recolector se haya propuesto para solicitarlos y obtenerlos, además de hace referenciar a cuál es el propósito por el cual el titular de los datos está dando su consentimiento para ser utilizados, según los casos en que este consentimiento corresponda por ley.

[24]VIOLLIER, P. (2017), *Op. Cit*.p.22

Es de extremada relevancia recalcar la dimensión del consentimiento en relación con este principio. El acuerdo entre las personas y el ente tratante de información es el que da cuenta de la manifestación de la voluntad del titular de los datos personales, quien es sujeto del derecho fundamental de la privacidad, para que el banco de datos u entidad que quiera realizar tal tratamiento tenga la autorización correspondiente en orden de realizar tal acto. Es la declaración del pensamiento del titular, que este se trasciende de sí mismo y se vuelve una expresión objetiva perceptible en la realidad,[25] y como tal es la que por regla general gatilla todo el proceso de utilización de la información del titular. Tomarse el derecho fundamental de la privacidad y el fundamento subyacente principio de finalidad en serio implica poder atender de manera adecuada el paradigma del consentimiento, y por ende del control que el individuo tiene (o debiese tener) respecto de su propia información. Este asunto al día de hoy con los avances digitales es cada vez más relevante. En suma, la relevancia del consentimiento radica en dar cuenta que el titular tiene el control de su información, y que dispone de mecanismos para poder administrarla según mejor le parezca en el contexto de su propio autogobierno.

Como ya se pudo analizar en las críticas a la ley de protección de la vida privada, no se exige en términos absolutos el consentimiento del titular para poder ejercer el tratamiento de datos personales. Una clara excepción a este respecto son los datos que provengan de fuente publica y los datos de carácter económico, financiero bancario y comercial. Si bien es cierto que estas excepciones son extremadamente amplia y difusas, existen ciertos argumentos que responden a consideraciones de eficiencia que apuntan a que el consentimiento no sea una excepción absoluta, pues tal como se ha dicho desde la doctrina, uno de los principales efectos que trae aparejado no tener esta exigencia, es la disminución de costos asociados al tratamiento.[26] Como podemos ver, este ahorro se vuelve muy relevante con la automatización del procesamiento de datos mediante algoritmos, que tal como ya vimos con anterioridad, hace que importante parte del tratamiento se realice sin consciencia del titular. Es aquí donde se puede notar una clara pugna en dos intereses contrapuestos: la protección de la vida privada versus la eficiencia en la gestión de datos (en especial en aquellos de carácter económico que muchas veces articulan el correcto funcionamiento de los mercados). Respecto de cómo superar este choque, se entrará en mayor detalle más adelante en este texto.

[25] VIAL, V. (2006). Teoría general del acto jurídico, 5ta Edición, Editorial Jurídica de Chile p. 48
[26] ALVARADO, F. (2014). *Op. Cit*. p. 218

Dicho todo esto, la ley recoge una visión más concreta en su artículo 9, al disponer que los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público. Acá podemos interpretar que, si el titular consciente que los datos deben ser utilizados únicamente para una determinada finalidad, entonces cualquier contravención a eso se constituye como una violación al artículo recién leído, configurándose de esta forma el principio de finalidad de manera un poco más explícita. El artículo establece en su segundo inciso un estándar relativo al contenido de la información que va a ser objeto del tratamiento, diciendo de que esta deberá ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos, estableciendo así una obligación por parte de quien realice el tratamiento de asegurarse que la información que se está manipulando tiene la característica de ser fidedigna. En seguida, en el artículo 10 se complementa lo dispuesto en la norma precedente respecto del principio de finalidad, al disponer que no pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares. De este modo, la ley dispone como norma general que los datos sensibles solo podrán ser manipulados cuando el titular de su consentimiento, lo cual leído sistemáticamente con el artículo 9 nos permite concluir que los objetivos particulares que el dueño de la información consienta para dar su información articularía el parámetro por el cual se pueden tratar estos datos, y por ende, como ya mencionamos, cualquier desviación que se escape de este parámetro se constituirá como una afectación de la intimidad del titular.

Este recogimiento del principio de finalidad guarda coherencia con lo dispuesto en el artículo 12 de la ley en análisis, que dispone a propósito de los derechos de los titulares, que estos podrán exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente. Así, toda persona puede exigir al banco que está almacenando sus datos que este le comunique con que propósito se están utilizando, con el objeto de constatar que se estén utilizando para la finalidad que fueron entregados en un inicio.

Hecho todo este análisis, cabe mencionar respecto de este estudio general respecto del principio finalidad que además de todo lo mencionado, se ha argumentado desde la academia que este se debe elevar a la categoría de ser un derecho subjetivo del titular de

estos, sosteniéndose que este dispone del derecho a un uso conforme a fin de los datos que le conciernen[27].Las implicancias jurídicas que esto o traería es de gran relevancia. Siguiendo a Ferrajoli, los Derechos Subjetivos son "toda expectativa jurídica positiva (de prestaciones) o negativa (de no lesiones)"[28], en este entendido, que la finalidad sea un derecho subjetivo implica que existe una expectativa de carácter jurídico por parte del titular de que los datos se van a utilizar con los fines para los cuales se presta el consentimiento, lo cual tendrá como consecuencia directa la posibilidad de hacer valer esta expectativa jurídica dentro de un determinado proceso judicial en caso de verse lesionada por algún tercero. Esta propuesta, sin embargo, difícilmente se puede lograr si no existe algún organismo que permita el hacer valer esta pretensión jurídica.

El gran problema que desde ya se puede notar a este respecto, es que como ya mencionamos cuando nos referimos a las críticas que se han hecho a la Ley de Protección de la Vida Privada, el consentimiento del titular no es requerido para poder hacer tratamiento de los datos de carácter financiero, económico, comercial o bancario, en concordancia con lo dispuesto en el artículo 4 de la ley. Esto trae como consecuencia lógica, que toda la eficacia que el principio de finalidad pueda revestir se ve erosionada, al no tener el titular un control suficiente respecto a cómo se van a utilizar sus datos pecuniarios. De este modo, esta situación se traduce en que la finalidad queda completamente determinada por la entidad que realizará el tratamiento de los datos, y que por lo tanto solo si se desapega de esa finalidad para la cual ella misma está incurriendo en la información económica del titular, se podrá alegar una infracción en virtud del principio de finalidad. En definitiva, esta situación es en extremo compleja, debemos recordar que la manifestación de la voluntad del titular es una expresión que da cuenta del respeto al derecho fundamental a la privacidad de las personas, el cual en definitiva se concretiza mediante el consentimiento, y sin este hito, la personalidad de los individuos se encuentra en serios riesgos de poder verse expuesta e incluso lesionada por parte del tratante de los datos, algo que en una sociedad democrática es inaceptable.

[27] CERDA, A. (2012). *Op. Cit.* p.27

[28] FERRAJOLI, L. (2000). "*Garantías"*, en Jueces para la Democracia, N°38. p. 40. En: CARBONELL, F. y LETELIER R., (2020) Debido proceso y garantías jurisdiccionales. En: Curso de Derechos Fundamentales. Editorial Tirant lo Blanch p. 356

III. Consolidación de la finalidad en materia económica y financiera. La ley N°20.575.

Ante la compleja situación recién expuesta en la cual se encuentran los datos pecuniarios, y circunscrito el contexto de la necesidad de poder consagrar de mejor manera el principio de finalidad a este respecto, es que durante el año 2012 entra en vigencia la ley N° 20.575, que "Establece el principio de finalidad en datos personales". Cabe mencionar que esta es la última gran reforma que se ha hecho en la materia,(sin contar la reforma constitucional al artículo 19 N°4 CPR, que tiene un carácter más bien simbólico) y por ende con la entrada en vigencia de esta ley es que se constituye prácticamente la totalidad de la regulación vigente de datos económicos al día de hoy. Tal como lo indica la historia de la ley, esta se encuentra enmarcada como una manera de responder de manera puntual las reiteradas críticas que en general la ley de protección de datos ha sido objeto, y en ese entendido la normativa tiene un fin claro: fortalecer el principio de finalidad, en materia de datos de carácter económico, bancario, comercial y financiero, estableciendo que será exclusivamente la evaluación de riesgo comercial y para el proceso de crédito, regulando las entidades a quienes se pueden comunicar estos datos y la forma en que sus titulares pueden acceder a ellos.[29] Este objetivo, responde a una problemática que también consta claramente en la historia de la ley, que es que en la época, existían cerca de 4 millones de personas se encuentran en los registros del DICOM por atrasos, moras o incumplimientos comerciales de distintas entidades; a juicio de la comisión "este sistema que es indispensable para la adecuada marcha de la economía y facilitar el acceso al crédito, ha desviado el propósito para el cual fue creado, esto es, evaluar el riesgo en el proceso de crédito."[30] Así, podemos ver como justamente en los hechos, la desviación del propósito para el cual eran recolectados los datos financieros de millones de personas en el sistema DICOM, las estaba dejando en un estado de indefensión al ser usada esta esta plataforma ya no como un mecanismo para evaluar el crédito de su persona y por lo tanto su capacidad de solvencia, sino como, una para practicas totalmente diferentes y perjudiciales para quienes constaban en tales registros. Un ejemplo de esto es que para acceder a un trabajo se consulte el DICOM del postulante y ello influya en la decisión de contratación.[31]

[29] CHILE, Congreso Nacional de Chile. Primer informe de la comisión de economía, que recae en el proyecto de ley en el segundo tramite constitucional en el Senado que establece el principio de finalidad en datos personales. p.4
[30] *Ibid.*
[31] *Ibid.* p. 5

No está demás mencionar que, con esta reforma, aún no se requiere del consentimiento del titular para poder realizar el tratamiento de datos, pero al menos especifica la aplicación del principio y vuelve mucho más preciso el mecanismo de determinación de la finalidad, lo cual hace que su aplicación en los hechos se vuelva más plausible, además de, como veremos, otorgar instancias en donde los titulares de los datos puedan alegar en caso de verse afectados por un quebrantamiento de la finalidad.

Las problemáticas que motivaron al legislador a promulgar esta normativa se puede relacionar a su vez con lo expuesto con anterioridad respecto a la falta de una capacidad en los hechos de la ley N° 19.628 de poder proveer en términos materiales una adecuada protección de esta información sensible, en especial considerando el importante poder económico que pueden tener las instituciones financieras y las demás entidades tratantes de datos personales interesadas en poder obtener información de las personas que ingresan en los registros como DICOM. Es de este modo, que esta ley busca perfeccionar y adecuar el principio de finalidad para información de carácter económico y financiero, la cual, desde la época de su entrada en vigencia en el año 2012, se estaba empezando a ver cada vez más inserta en el mundo digital y con medios de pago electrónicos, los cuales por un lado resultaban mucho más expedito a la hora de concretar transacciones y negocios, y por otro lado implicaba la utilización de datos de los usuarios para poder lograrse.

Es por todo esto, que resulta del todo coherente que apenas uno se aproxima a este cuerpo normativo, ve que en su primer artículo se hace en seguida una referencia al ya mencionado Título III de la ley N° 19.628, que como vimos regula los datos de carácter económico, financiero, bancario o comercial. En este entendido, la norma en análisis nos indica que deberá respetarse el principio de finalidad en el tratamiento de datos personales, el que será exclusivamente la evaluación de riesgo comercial y para el proceso de crédito. En esta norma podemos apreciar la clarificación de este principio, al volver mucho más precisa su aplicación y al explicitar bajo que motivo se aceptará el tratamiento (evaluación del riesgo comercial y el proceso de crédito). En su segundo y tercer inciso, se declara que la comunicación de esta clase de datos sólo podrá efectuarse al comercio establecido, para el proceso de crédito, y a las entidades que participen de la evaluación de riesgo comercial y para ese solo fin. Finalmente, en su último inciso, dispone que en ningún caso se podrá exigir esta información en los procesos de selección personal, admisión preescolar, escolar o de educación superior, atención médica de urgencia o postulación a un cargo público. Este último inciso claramente es una respuesta expresa a las problemáticas que previamente se

expusieron en torno al erróneo uso que ciertas personas estaban dándole a registros como DICOM, al utilizar la información que consta en esta clase de base de datos en orden de impedir el acceso a servicios públicos y trabajos a los deudores, lo cual evidentemente ya no solo se constituye como una vulneración a la privacidad, sino a un sinnúmero de otros derechos fundamentales vigentemente consagrados en nuestra Constitución, como la integridad física y psicológica o el acceso a la educación.

De este artículo de la Ley N° 20.575, podemos ver que el principio de finalidad no solo se explicita en materia económica, sino que se especifica de manera muy notable, al ya no solo hacer referencia a lo que se considere como licito en la Ley de Protección de la Vida Privada, sino que se establecen de manera expresa finalidades que son derechamente ilícitas a los ojos del legislador, por perjudicar a los usuarios de una manera multidimensional al no permitirles acceder a servicio tan elementales como la atención médica o a instancias fundamentales como la educación en sus diversos niveles. Este ajuste normativo en suma permite impedir que los consumidores y titulares de datos personales se encuentren en un estado de indefensión en determinadas situaciones recogidas por ley, sin embargo, esto no pareciera ser suficiente para poder dar una protección desde una perspectiva holística de la privacidad en términos económicos. Pues tal como lo pudimos apreciar en lo dicho en la tramitación de esta ley, el objetivo era resolver problemas específicos que se estaban dando al respecto de determinados registros, mas no encontrar una solución que pueda dar mejores garantías a las personas en términos universales. A mayor abundamiento, un modo en que se ha propuesto desde la doctrina para afrontar estas dificultades (particularmente las bases de datos de deudores) de mejor manera es la implementación de un sistema de información crediticia mixto, lo cual se traduce en que el registro se componga por tanto las deudas cumplidas como las incumplidas,[32] de modo de que la capacidad de solvencia se vea desde una perspectiva más amplia, y que impida que se solo se vea la faz negativa del registro, lo cual lograría evitar que el titular se vea perjudicado a la hora de postular a servicios, trabajos, beneficios, etc. Hoy en día el sistema de información crediticia es solo negativo, lo cual es tributario de todos los problemas que hemos analizado.

En definitiva, podemos ver como en esta ley el principio de finalidad se constituye como un estándar de comportamiento esperable respecto de entes que se encuentran facultados para hacer uso de los datos personales de los particulares para determinados fines. Es en observancia de justamente esta consideración, que en su artículo segundo, se define quienes

[32] Véase BOZZO, S. (2020).*Op. Cit.* pp. 120-122

serán estos entes responsables del tratamiento de datos, entendiendo para efectos de la ley que son distribuidores de información de carácter económico, financiero, bancario o comercial, las personas naturales o jurídicas que realizan directamente el tratamiento, comunicación y comercialización de los datos de obligaciones económicas, de conformidad con lo dispuesto en la legislación vigente y con pleno respeto a los derechos de los titulares de los datos. Así, no solo se cristaliza el estándar de comportamiento esperable en la materia, sino que caracteriza quienes serán las personas responsables de cumplir con este principio de finalidad, siendo entonces una desviación o quebrantamiento ilícito de tal estándar hacer uso de estos para cualquier otro fin que no sea el acordado con el usuario.

Además de todo esto, es relevante mencionar que esta ley intenta mitigar un poco los problemas que la ley N°19.628 ha tenido, estableciendo en su artículo número cuatro que los distribuidores de los registros o bancos de datos personales de carácter económico, financiero, bancario o comercial, deberán designar a una persona natural encargada del tratamiento de datos, de manera que los titulares de datos puedan acudir ante él para los efectos de hacer efectivos los derechos que les reconoce la Ley sobre Protección de la Vida Privada. En definitiva, se constituye un mandato a estas entidades de poder facilitar que los titulares tengan un modo de poder hacer efectivos sus derechos fundamentales de privacidad en caso de cualquier entorpecimiento que pueda existir en referencia a su información pecuniaria personal. Si tomamos en consideración las pocas instancias que en la actualidad hay en nuestro país para reclamar esta clase de vulneraciones, es innegable de que esto es un aporte valioso.

Como podemos ver, esta ley es un importante avance en poder adecuarnos a la realidad del tráfico de información que ya desde la época en que fue tramitada se estaba empezando a dar y así poder dar cuenta de una red de resguardo que se encuentre a la altura de las circunstancias. No obstante lo anterior, y tal como la historia de la Ley lo indica, y como en este texto también se ha mencionado ya, esto es definitivamente una normativa que es destinada a resolver un problema particular que por lo demás requería de una solución urgente, sin embargo, no basta para por un lado, poder decir que nuestro país se encuentra en concordancia con cómo se ha atendido el problema en la legislación extranjera contemporánea la materia, y por otro, mucho más importante, afirmar que tenemos un sistema que realmente proteja la vida privada en términos generales, y particularmente los datos financieros de un modo adecuado.

Es por todo esto que a continuación se hará un estudio y análisis detallado de cómo se ha enfrentado esta materia y los estándares aplicables en el ámbito internacional, haciendo un especial énfasis en la legislación de la Unión Europea y la de organizaciones supranacionales como la Organización para la Cooperación y el Desarrollo Económicos (de ahora en adelante, OCDE).

CAPÍTULO 3: Principios y legislación referente a la finalidad de los datos personales en el ámbito Internacional: evolución y desarrollo

I. La discusión de la protección de los datos personales en el ámbito internacional

Desde que comenzó a existir legislación al respecto, durante la segunda mitad del siglo XX, la protección de datos personales ha evolucionado y actualmente es posible encontrarla en distintos ordenamientos jurídicos. Asimismo, cabe mencionar que este fenómeno también se ha manifestado en el panorama supranacional mediante diferentes organizaciones de cooperación entre Estados. Desde esta perspectiva podemos apreciar que han existido diversos esfuerzos legislativos para ir perfeccionando la normativa referente al tratamiento de todo lo relacionado a informática y datos en términos generales. Ahora bien, es relevante destacar que esta es una discusión de mucha más larga data en el ámbito internacional (especialmente en Europa y Norteamérica) en comparación con nuestro país. Así, por ejemplo, en la Alemania Federal las primeras legislaciones se promulgaron durante la década de los 70', y en Estados Unidos de América vemos un primer esfuerzo con la *Privacy Act* de 1974. Desde entonces, como hemos mencionado previamente, ha existido una evolución constante en la materia lo que ha ocasionado que hoy existan una gran variedad de sistemas para regular los datos personales. En este sentido, y en consonancia con algunos de los temas que se han tocado a lo largo de esta monografía, podemos ver que en Francia la información crediticia se trata por medio de un registro público[33], en contraste con la regulación de Países Bajos, donde ni siquiera hay una referencia expresa a la regulación crediticia en su respectiva ley de protección de datos.

A propósito de la normativa supranacional de datos personales, es relevante mencionar que una de las primeras expresiones en esta materia viene por parte de la OCDE. Esta organización aprobó el día 23 de septiembre del año 1980 el primer instrumento que intentó reglamentar el procesamiento de datos personales y, particularmente, el flujo internacional de dichos datos. Este instrumento se constituyó por una serie de directrices relativas a la protección de la intimidad. Así, con esta promulgación se buscaba por un lado promover la democracia, el respeto por los Derechos Humanos y la economía de libre mercado, mientras que por otro, se buscaba establecer un estándar mínimo en miras de promover la armonización

[33] Este registro se conoce como el registro público de solvencia (*Service Central des Risques*), el cual fue creado el año 1946, entrando en funcionamiento ese mismo año.

internacional de las normas relativas al tratamiento manual y automatizado de información personal por los sectores público y privado[34].

Por su parte, los países europeos también han tenido la característica de no mantenerse indiferentes ante la materia en estudio. Pues, prácticamente de manera contemporánea a las primeras directrices de la OCDE, durante el año 1981 se llevó adelante por parte del Consejo de Europa, el "Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", también conocido como "Convenio de Estrasburgo". Tal como se indica en el primer artículo del Convenio, su objeto y fin es el de garantizar el respeto de derechos y deberes de las personas físicas, derecho a la vida privada con respecto al tratamiento automatizado de sus datos de carácter personal. Si bien sus disposiciones son principalmente aplicables a personas físicas, tal como lo indica el artículo primero, un país parte también podría aplicar lo dispuesto por el Convenio a personas jurídicas, en concordancia con lo dispuesto en el artículo tercero.

No obstante, pese a que se puede afirmar que este Convenio es un hito de gran importancia en el avance de una normativa que involucre la cooperación simultánea de muchos países para mejorar la protección de la intimidad, su contenido devino en insuficiente para poder atender las problemáticas asociadas a este fenómeno, así como lo relativo al uso transfronterizo de datos personales[35]. Por esta razón la Unión Europea continuó en su esfuerzo de generar una integración de la regulación del flujo de información sensible de las personas naturales y físicas, emanando así nuevas directivas, reglamentos y convenios, como la Directiva 95 N°95/46/CE del Parlamento Europeo y del Consejo, (de ahora en adelante, Dir. 95) relativa a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta directiva se ve enmarcada en la iniciativa de materializar una regulación comunitaria vinculante para todos aquellos países miembros[36]. Es claro que con la llegada del siglo XXI, y los desafíos que este trae junto con la necesidad de perfeccionar y actualizar la normativa para afrontar las nuevas dificultades, los estándares internacionales han debido ir adecuándose.

De esta manera, podemos ver cómo el desafío del resguardo de la información personal de las personas es una problemática constantemente evolucionando. Fiel reflejo de aquello es que se ha visto modificada en constantes ocasiones y ha ido generando diferentes

[34] CERDA, A. (2011). El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la unión europea". *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, (36). p. 326.
[35] *Ibid*. p. 330.
[36] *Ibid*. p. 331.

parámetros respecto de los cuales los países deben actuar para que la protección de datos sea percibida como un mecanismo realmente eficaz.

Es en este contexto, que, volviendo al panorama de nuestro país, podemos ver que luego de la promulgación de la mencionada ley N° 20.575 durante el año 2012 que, como se mencionó en su momento, se reportaron mejoras para intentar resolver problemas relacionados a la implementación del principio de finalidad. Los estándares han ido replanteándose alrededor del mundo y evolucionando para adecuarse, en términos generales, a las circunstancias que envuelven el panorama de los datos personales llegando así a los desafíos de la actualidad, que vienen de la mano con un agigantado y dinámico avance tecnológico que se ha experimentado desde las telecomunicaciones, las plataformas digitales, entre otros. Aquí es donde podemos apreciar que no se han promulgado nuevas reformas profundas y estructurales que estén a la altura de este mundo digital, lo cual ha traído como consecuencia inmediata que nuestra legislación, que ya presentaba desde un principio importantes deficiencias, resulte deficiente. La última reforma relevante a esta cuestión fue la modificación del artículo 19 N° 4 de nuestra Constitución Política, que más que crear un entramado normativo que permita afrontar la era digital, se muestra más bien como una tardía muestra de sensibilidad por los datos personales que tiene un peso mucho más simbólico que concreto. En definitiva, si bien ciertas carencias denunciadas desde la publicación de la Ley N° 19.628 se fueron colmando con reformas puntuales, de todas maneras, se extraña en el derecho positivo chileno una reforma de carácter integral que adapte su régimen jurídico a la evolución social y económica del flujo de datos, con una amplia participación social, no solo del mundo empresarial, sino que también de la doctrina y de la academia[37].

En contraste, como ya se ha expuesto, en otras latitudes sí se ha tomado en serio este desafío y se han ido presentando en reiteradas ocasiones nuevas normativas y directrices para adecuar el régimen de protección de datos, siendo las últimas versiones de estos cuerpos muy contemporáneos. Un gran ejemplo son los reglamentos de la Unión Europea o los lineamientos actualizados de la OCDE que veremos a continuación en el siguiente apartado. En estos documentos se podrá apreciar que el principio de finalidad ha experimentado modificaciones que van en la línea de las evoluciones que hemos expuesto.

[37] BAUZÁ, F. (2019). El modelo europeo de protección de datos. Experiencias para la regulación chilena presente y futura. *Ars Boni et Aequi*, *15* (1), p. 124.

II. Los cuerpos normativos supranacionales contemporáneos de protección de datos personales de cara al principio de finalidad

A) El Reglamento 2016/679 de la Unión Europea (RGPD)

Concretamente, el principio de finalidad desde hace décadas ha sido un tema de preocupación para el parlamento europeo. Esto resulta evidente ya en el artículo sexto letra b) de la Dir. 95 se dispone que los estados miembros de la directiva deberán disponer de los datos sean recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines. La norma establece la excepción de que no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas. Estas garantías, evidentemente, son de total importancia, pues por un lado ayudan a delimitar el ámbito de aplicación del tratamiento de datos, y por otro, dota de elementos a los titulares que permitan la tutela de sus derechos. De este modo, la directiva establece una noción de finalidad mucho más concreta que la que se recoge en términos generales en nuestra ley N° 19.628, agregando criterios de legitimidad y explicitud a la hora de recoger los datos, lo cual ya nos habla de una mayor robustez regulatoria de los datos personales en comparación con la ley vigente en Chile, además de establecer este mandato de garantías a los Estados miembros. Es relevante recordar que el artículo noveno de esta ley dispone como norma general que los datos personales deben utilizarse solo para los fines para los cuales hubieren sido recolectados. Realizándose una lectura sistemática de la ley, solo se podría complementar con que estos fines sean concordantes con la ley misma y el ordenamiento jurídico en general, sin dar muchas más luces de la caracterización de la finalidad en el tratamiento de la información, además de, como ya se ha mencionado reiteradas veces, establecer amplias excepciones con garantías que no dan cuenta de un real sistema de protección para los titulares de la información.

Como hemos indicado anteriormente, la necesidad de ir reinventando la normativa que atiende a la protección de la intimidad, en atención a como el panorama informático va evolucionando de la mano de la tecnología, es una que en materia de legislación supranacional se ha mantenido constantemente en la palestra. Por esta principal razón vemos que la normativa vigente en la materia para Europa es bastante reciente. Este es el caso del Reglamento 2016/679 del Parlamento Europeo (en adelante, RGPD), promulgado el día 27 de

abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Así, podemos apreciar como en el considerando [13] del reglamento, se diagnostica que para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es absolutamente necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y que además ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades.

Para efectos del análisis de cómo se regula el principio de finalidad en este cuerpo normativo, y recalcando la gran importancia que se le ha dado a lo largo de este ensayo, es que resulta muy notable apreciar cómo se presenta el tópico del consentimiento al interior de este reglamento. A este respecto, el RGPD apuesta por una aceptación expresa y afirmativa del consentimiento. De este modo, en su considerando [32] se dispone lo siguiente:

> *"El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta".*

Por estas mismas consideraciones, es que el artículo 4.11 del Reglamento define el consentimiento como "toda manifestación de voluntad libre, especifica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara afirmación afirmativa, el tratamiento de datos personales que le conciernen".

Cabe observar que al definir expresamente qué es consentimiento aquí ya se resuelve una incerteza presente en nuestro ordenamiento, lo cual permite que toda regulación posterior devenga en ser más certera. A su vez, es muy importante advertir que la caracterización del consentimiento es muy concreta, entendiéndose como tal una expresión de voluntad libre, informada e inequívoca, en contraste con la referencia que hay en nuestra Ley de Protección de Datos, donde solo se da cuenta de la necesidad de que el consentimiento sea expreso y por escrito. En este sentido, ha sido un acierto considerar que un consentimiento expreso no equivale a un consentimiento libre, o uno que presente las demás características que se consagran en el RGPD.[38] En referencia a las excepciones al consentimiento, solo se puede observar que en el contexto de la soberanía y autodeterminación nacional, estas dependerán de cada país miembro de la Unión Europea. Toda esta normativa referente al consentimiento es una variable fundamental para un sistema que ofrece garantías concretas al titular, por cuanto se establece como un verdadero reconocimiento de la autonomía de los individuos y de lo que viene aparejado respecto de su intimidad y autogobierno, por lo cual estimamos que es una aproximación general adecuada, sin perjuicio de las excepciones que por diferentes motivos se puedan discutir en cada país.

Ateniéndonos ahora a la regulación expresa de la finalidad en el Reglamento, advertimos que, al igual que en la Dir. 95, se recogen en un inicio una serie de principios a los cuales debe responder cualquier acto en el que se vean involucrados datos relacionados con la privacidad de las personas y su respectivo tratamiento. Entre estos principios, destaca el contemplado en el artículo quinto número 1. b), el cual fue redactado con una técnica legislativa muy similar a la del artículo 6 b) de la Dir. 95. La norma en análisis dispone que los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. La norma también agrega que, en concordancia con lo dispuesto el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales. La diferencia más importante que se puede encontrar en la redacción de este artículo con el de la Dir. 95 es la cláusula que se dejó escrita al final entre paréntesis, una indicación que dispone la frase “limitación de la finalidad”. Con esta última terminología se recoge un nuevo estándar de tratamiento de datos que, como veremos, presenta ciertos matices respecto a las características típicas al principio de finalidad que se encuentra actualmente recogido en

[38] *Ibid*. p. 128.

nuestra legislación vigente, y cuyas consecuencias jurídicas y normativas son del todo relevantes.

Según la Agencia Española de Protección de Datos la limitación de la finalidad implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.[39] De este modo, y tal como su nombre lo indica, la finalidad en este caso quedará limitada no solo respecto a parámetros que responden a consideraciones de legitimidad y licitud, sino a compatibilidad del propósito para el cual se están utilizando. Esto, como veremos, trae consigo que en materia de datos económicos financieros se pueda crear un método de protección mucho más flexible ante el consentimiento del titular y que permita una determinación de la desviación de la utilización de datos que resulte mucho más exacta.

En este entendido, y teniendo siempre en consideración de que estamos analizando la finalidad referente a datos de carácter económico y financiero, es que resulta del todo relevante lo dispuesto en el artículo 47 del reglamento, el cual consagra la regulación atingente a las normas corporativas vinculantes. En esta norma en particular, se dispone que la autoridad de control competente podrá aprobar normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido por el mismo reglamento en la medida en que se cumplan con una serie de requisitos. El primero de estos requisitos es que estas normas corporativas sean jurídicamente vinculantes, se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados. En segundo lugar, que confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y finalmente, en tercer lugar, que se cumpla con el listado de requisitos dispuestos en el segundo apartado del artículo en análisis. En este segundo apartado se dispone en su letra d) como requisito para la implementación de esta normativa corporativa, la aplicación de los principios generales en materia de protección de datos, en particular, la limitación de la finalidad.

En este artículo se puede apreciar otro paradigma, aquel donde la regulación de los datos personales resulta del todo relevante, en donde ya no nos aproximamos a la

[39] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2021) Principios. Disponible [en línea]: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios [Consulta: 6/2/22].

problemática desde la perspectiva de los consumidores y deudores, sino que desde la perspectiva del gobierno corporativo interior de las empresas, y del deber de administrarlas siempre en orientación de cumplir con los principios fundamentales, como la finalidad. Este paradigma de suma se constituye como un pilar fundamental para que aquellas personas jurídicas que se desempeñen como tratante de datos cuenten con un régimen interior vinculante, en orden de que se respete la normativa vigente y los principios fundamentales referentes a la protección de datos.

De este modo, el reglamento no solo declara como principio general la limitación de la finalidad, sino que además, en caso de que los Estados miembros busquen realizar normas de carácter corporativo, se deberá redactar la normativa considerando transversalmente la limitación de ella. Lo cual hace que se asegure que el principio esté presente en cualquier tratamiento de información sensible de carácter económico, regulándose de forma integral la observancia de los estándares que deben reportarse en la finalidad de cualquier cuerpo normativo que sea relevante para la materia en estudio.

Finalmente, respecto del RGPD vale la pena destacar una serie de medidas de seguridad que este reglamento impone a los Estados miembros en orden de hacer valer la protección de los datos personales en general, logrando de este modo que principios como el de finalidad se hagan cumplir como corresponde. Por consiguiente, estas medidas se erigen como un mecanismo para asegurar que esta regulación se concretice.

Al respecto, se ha afirmado que el RGPD opta por una estrategia de seguridad que gira esencialmente en torno a la noción de riesgo[40]. En tal sentido, aquel riesgo debe ser objeto de evaluación previa atendiendo la naturaleza, el alcance, el contexto y los fines del tratamiento de datos[41]. Es en este entendido que el reglamento introduce la noción de responsabilidad y autoridad de control en orden de poder dar seguridad en el tratamiento de los datos. La implementación de esto se puede ver en parte del articulado del RGPD, entre los artículos más importantes, se pueden encontrar los siguientes:

1) El artículo 32 del reglamento, que impone que el responsable y el encargado del tratamiento tendrán el deber de implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: a) el cifrado y caracterización de anonimato de los datos; b) la

[40] MALDOFF,G. (2016). The Risk-Based Approach in the GDRP: Interpretation and Implications. Disponible [en línea]: https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf [Consulta: 6/2/22]
[41] BAUZÁ, F. (2019). *op. cit*. p. 131

capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; y d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2) El artículo 33, que regula la notificación de violación a la seguridad de los datos personales a la autoridad de control, la cual, en palabras del propio artículo, no podrá demorar más de 72 horas.
3) El artículo 34, que regula la notificación de violación de seguridad de los datos personales al interesado. Esta se debe realizar en un lenguaje claro, y sin dilaciones indebidas, comunicando la naturaleza de la violación de la seguridad de los datos personales.
4) El artículo 35, que regula la evaluación de impacto relativa a la protección de datos. Esta evaluación es clave, y da cuenta no solo de los avances que este reglamento reporta en la regulación y protección de la privacidad de las personas, sino que realiza un análisis prospectivo en relación a los eventuales futuros desafíos que se presenten en el futuro. De este modo, el artículo dispone en su primer apartado que cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento deberá realizar, antes del tratamiento propiamente tal, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. En definitiva, dando cuenta de esta estrategia de regulación basada en los riesgos, se busca mitigar perjuicios a los titulares haciendo evaluaciones *ex ante* del impacto que puede traer el implementar determinados tipos de tratamiento, en especial si nuevas tecnologías se ven involucradas.
5) Finalmente, el artículo 36, muy de la mano con el previo, regula un procedimiento de consulta previa ante la autoridad de control. Así, se dispone que el responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos, en virtud del artículo 35, muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo. A su vez, este artículo establece en sus siguientes apartados una serie

de medidas que podrá tomar la autoridad de control en caso de que el responsable no haya identificado o mitigado suficientemente el riesgo.

En definitiva, con estas medidas de seguridad, y con toda la normativa de fondo respecto de la noción de consentimiento y de limitación de la finalidad, es que se puede apreciar un verdadero entramado normativo que da cuenta de medidas tanto *ex ante* como *ex post* para poder resguardar la privacidad de las personas ante las entidades que realizan tratamiento de datos, y que, dejando procedimientos claros, permite que los datos sean utilizados de manera segura, y aún más importante, que el titular mediante su personalidad y autonomía, tenga un auténtico control de su propia información.

B) La regulación de la protección de la vida privada y del principio de finalidad en la OCDE

Lo primero que vale la pena recalcar en esta sección, es que tal como lo indica el artículo primero del Convenio firmado el 14 de diciembre de 1960 en París, entrado en vigor el 30 de septiembre de 1961, la Organización para la Cooperación y el Desarrollo Económico (OCDE) tiene por objetivo promover políticas dirigidas a:

- Conseguir la mayor expansión de la economía y el empleo, y una progresión del nivel de vida en los países miembros, manteniendo la estabilidad financiera, y así contribuir al desarrollo de la economía mundial.
- A contribuir a una sana expansión económica en los países miembros, así como en los países no miembros, en vías de desarrollo económico.
- A contribuir a la expansión del comercio mundial sobre una base multilateral y no discriminatoria, conforme con las obligaciones internacionales.

Asimismo, a través de principios básicos y fundantes de la Organización se ha impuesto el deber de poder contribuir con el comercio mundial en miras del desarrollo económico, pero siempre persiguiendo un equilibrio con las obligaciones internacionales que le conciernen, entre las cuales se encuentra el respeto de los derechos humanos básicos de las personas. Como ya se mencionó en su momento, al interior del catálogo de derechos que contempla la Declaración Universal de Derechos Humanos, existe una disposición (el artículo 12) que indica que nadie podrá ser 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. De este modo, entre las

obligaciones internacionales que se deben ponderar a la hora de contribuir al sano crecimiento económico y del comercio mundial, se encuentra el respeto a la no injerencia a la vida privada de las personas.

Las regulaciones, indicaciones y directrices supranacionales de la OCDE resultan de mayor sensibilidad para nuestro país si las comparamos con las de la Unión Europea, por cuanto, a diferencia de esta última organización internacional, Chile sí es parte de la primera, y por lo tanto, tiene la responsabilidad y el deber de hacer seguimiento a estos estándares. Desde el año 2010 nuestro país es parte de esta organización de cooperación, y tal como se ha indicado desde la literatura, para convertirse en miembro Chile ha debido demostrar que está dispuesto a aceptar (*willingness*) y comprometerse a asumir (*ability*) las obligaciones y recomendaciones contenidas en los instrumentos OCDE, así como los estándares, directrices, *benchmarks* y principios rectores establecidos por la Organización[42]. Es por todo esto, que la normativa de datos personales y los principios que sigue la OCDE siempre son de relevancia para nuestra legislación nacional, al ser los estándares que nos hemos comprometido a seguir a la hora de haber aceptado ser parte de esta organización.

Por otra parte, es muy importante recalcar que durante el año 2013 las directrices de datos personales de la OCDE fueron actualizadas siguiendo la lógica ya expuesta de la necesidad de constante evolución y reinvención de esta normativa. De esta manera, se ha avanzado hacia una adecuación a los desafíos tecnológicos del siglo XXI de los cuales ya hemos hecho referencia en este texto en reiteradas ocasiones. Y es en este mismo entendido que las directrices reconocen esta vocación evolutiva desde su preámbulo, afirmando que el tratamiento automático y los flujos transfronterizos de datos personales crean nuevas formas de relaciones entre los países y requieren la elaboración de normas y prácticas compatibles[43]. En definitiva, es por esta misma razón que la primera recomendación de este cuerpo es, justamente, que los Países Miembros tengan en cuenta para su legislación interna los principios relativos a la protección de la privacidad y las libertades individuales establecidos en las Directrices contenidas en el Anexo a esta Recomendación, y que forma parte del mismo[44].

[42] SZCZARANSKI, C. (2011). *Un asunto criminal contemporáneo. Rol de las empresas, responsabilidad penal de las personas jurídicas y corrupción*. Santiago, Chile. Editorial Jurídica de Chile. p 223.
[43] Véase: OCDE. (2013). Directrices sobre la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales. Disponible [en línea]: https://www.oecd.org/sti/ieconomy/15590267.pdf
[44] *Ibid*.

A propósito de estas directrices, distinguimos que la noción de finalidad se desprende principalmente de dos apartados. Por un lado, podemos identificar el apartado noveno, que dispone el denominado “principio de especificación de los fines”. Este principio, según el tenor de las directrices, se traduce en que los fines para los que los datos personales se recogen deberían especificarse en el momento en que son recogidos, y su uso posterior estaría limitado al cumplimiento de esos fines, o de otros que no sean incompatibles con estos, y a su vez, que se especifiquen cada vez que haya un cambio de fines. Por otro lado, está el denominado “principio de limitación de uso”, consagrado en el apartado décimo de las directrices, que dispone que los datos personales no se deberían revelar, poner a disposición del público ni usar para fines que no sean los especificados de conformidad con el apartado noveno anterior, excepto:

a) con el consentimiento del sujeto de los datos; o
b) por imperativo legal.

De estos dos apartados podemos apreciar que, en el caso de la normativa supranacional de la OCDE, también existe una preocupación por impedir la vulneración de los derechos de los titulares de datos en aquellos casos en que el tratamiento se desvíe de su propósito original. Por consiguiente, la finalidad solo puede ser modificada por mandato de la ley o el consentimiento, erigiendo así una obligación por parte de la entidad tratante que debe ceñirse estrictamente a estos parámetros.

Para la efectividad de estos principios corresponde, a su vez, el consignar otros que resultan de total relevancia para complementar su aplicación. En primer lugar, encontramos en el apartado número once el principio de salvaguarda de seguridad, que dispone que los datos personales deberían estar protegidos por las oportunas medidas de salvaguarda contra riesgos como pérdida o acceso no autorizado, destrucción, uso, modificación o revelación de datos. El otro principio relevante es el principio de transparencia, consagrado en el considerando doce, que se refiere a que los Estados miembros deberían tener una política general de transparencia en lo concerniente al tratamiento, el uso y las políticas relativos a los datos personales. Además, se indica que se deberían disponer los medios para establecer la existencia y la naturaleza de los datos personales, así como los fines principales para los que se van a usar, así como la identidad y el domicilio habitual del inspector de datos. Con estos principios se busca que la utilización y tratamiento de la información no solo estén en concordancia con las finalidades que se tenían originalmente, sino que también existan garantías de que tal gestión cumplirá con estándares de probidad y transparencia que den

cuenta de que se está cumpliendo con los parámetros legales; lo cual además es un antecedente importante para poder dotar de legitimidad el tratamiento de datos.

En suma, es la combinación de todas estas variables las que establecen una hoja de ruta para las naciones que son parte de la OCDE para que estos promulguen por la vía legislativa estándares y normativas de su derecho interno que tengan en el ámbito de la protección de datos un ámbito de aplicación bien delimitado, y con estructuras capaces de poder velar por la seguridad, la autonomía y los Derechos Fundamentaos de los titulares de datos personales.

Del análisis que ya se ha hecho de nuestra Ley de Protección de la Vida Privada del año 1999, y de la posterior y escasa legislación que se ha realizado en nuestro país desde entonces, se puede desprender claramente que Chile se encuentra muy al debe en estos aspectos, al tener normas cuya aplicación no es del todo clara y carecer de organismos con la suficiente idoneidad para dar una protección adecuada. En contraste, tanto la normativa supranacional vigente hoy en día en la Unión Europea, como la de la OCDE, da cuenta de indicaciones, principios y organismos que presentan una mayor eficacia a nuestra legislación en esta materia.

CAPÍTULO 4: El futuro de la normativa en Chile y sus correspondientes desafíos

I. Proyecto de Nueva Ley de Datos Personales

Como se pudo concluir al final del capítulo anterior (y en general a lo largo de este texto), en nuestro país tenemos una legislación a cargo de proteger la vida privada que ha sido y continúa siendo muy criticada en el medio nacional y que, en comparación con los estándares que han surgido internacionalmente durante los últimos años, resulta del todo insuficiente para poder hacerse cargo de los problemas que se presenta en materia de privacidad y datos personales, donde tenemos un principio de finalidad que requiere ser más específico para que logre tener una eficacia deseada y aceptable. Por esta razón el Congreso de nuestro país, durante el año 2017, gatilló un proceso de tramitación de una nueva Ley de Datos Personales. Con esto se busca tomar medidas de alcance general ante la obsolescencia de nuestro ordenamiento frente a esta materia, y de este modo aproximarnos a los principios recogidos internacionalmente, y resolverse de una vez por todas de las controversias que han sido objeto de la normativa vigente en Chile. Este proyecto de ley continúa siendo tramitado en la actualidad.

Ante este diagnóstico, principalmente dilucidado en el contexto de la discusión parlamentaria, se ha previsto para este nuevo proyecto la misión de perfeccionar las normas relativas al tratamiento de los datos personales de las personas naturales, de manera tal que se realice siempre con el consentimiento del titular de dichos datos o en los casos que lo autorice la ley, asegurando estándares de calidad, información, transparencia y seguridad[45]. Evidentemente, se puede apreciar que existe una preocupación por hacerse cargo de manera general de los problemas que se le ha criticado a nuestra actual ley por décadas y no solo de problemáticas puntuales. Asimismo, se busca crear la Agencia de Protección de Datos Personales, organismo público encargado de velar por la protección de esta clase de datos. Ante esto, en el Senado se ha entendido que existen una serie atribuciones y funciones que necesariamente deberá tener este organismo en orden de poder brindar mecanismos para que las personas puedan proteger su información ante lesiones a la intimidad ejercida por terceros, además de ser un aporte para el mejoramiento de la institucionalidad referente a esta materia.

[45] CHILE. Congreso Nacional de Chile. (2017). Informe de la comisión de constitución, legislación, justicia y reglamento recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. p. 5.

Tales atribuciones se pueden encontrar actualmente en el texto de la nueva ley que se está proponiendo en su artículo 30 bis, y son las siguientes[46]:

> *"Artículo 30 bis.- Funciones y atribuciones de la Agencia. La Agencia tendrá las siguientes funciones y atribuciones:*
>
> *a) Dictar instrucciones y normas generales y obligatorias con el objeto de regular las operaciones de tratamiento de datos personales conforme a los principios establecidos en esta ley. Las instrucciones y normas generales que dicte la Agencia deberán ser emitidas previa consulta pública efectuada a través de la página web institucional y deberán estar relacionadas estrictamente con la regulación de tratamiento de datos personales y que sea necesaria para el fiel cumplimiento de la presente ley, disponiéndose los mecanismos necesarios para que los interesados puedan formular observaciones a esta.*
>
> *b) Aplicar e interpretar administrativamente las disposiciones legales y reglamentarias en materia de protección de los datos personales y las instrucciones y normas generales que dicte la Agencia.*
>
> *c) Fiscalizar el cumplimiento de las disposiciones de esta ley, sus reglamentos y las instrucciones y normas generales que se dicten respecto de los tratamientos de datos personales. Para ello, podrá requerir a quienes realicen tratamiento de datos personales la entrega de cualquier documento, libro o antecedente y toda la información que fuere necesaria para el cumplimiento de su función fiscalizadora.*
>
> *d) Determinar las infracciones e incumplimientos en que incurran quienes realicen tratamiento de datos personales, en sus operaciones de tratamiento de datos, respecto de los principios y obligaciones establecidos en esta ley, sus reglamentos y las instrucciones y normas generales que emita la Agencia. Para tales efectos, y de manera fundada, podrá citar a declarar, entre otros, al titular, a los representantes legales, administradores, asesores y dependientes de quien trate datos personales, así como a toda persona que haya tenido participación o conocimiento respecto de algún hecho que sea relevante para resolver un*

[46] CHILE. Congreso Nacional de Chile. (2021). Informe de la comisión de hacienda recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletines N° 11.092-07 y 11.144-07, refundidos. pp. 186- 188.

procedimiento sancionatorio. Asimismo, podrá tomar las declaraciones respectivas por otros medios que aseguren su fidelidad.

e) Ejercer la potestad sancionadora sobre las personas naturales o jurídicas que traten datos personales con infracción a esta ley, sus reglamentos y a instrucciones y normas generales dictadas por la Agencia, aplicando las sanciones establecidas en la presente ley.

f) Resolver las solicitudes y reclamos que formulen los titulares de datos en contra de quienes traten datos personales con infracción a esta ley, sus reglamentos o las instrucciones y normas generales dictadas por la Agencia.

g) Desarrollar programas, proyectos y acciones de difusión, promoción e información a la ciudadanía, en relación al respeto a la protección de sus datos personales.

h) Proponer al Presidente de la República y al Congreso Nacional en su caso, las normas legales y reglamentarias para asegurar a las personas la debida protección de sus datos personales y perfeccionar la regulación sobre el tratamiento y uso de esta información.

i) Prestar asistencia técnica, cuando le sea requerida, al Congreso Nacional, al Poder Judicial, a la Contraloría General de la República, al Ministerio Público, al Tribunal Constitucional, al Banco Central, al Servicio Electoral, a la Justicia Electoral y los demás tribunales especiales creados por ley, en la dictación y ejecución de las políticas y normas internas de estos organismos, con el objeto que sus operaciones y actividades de tratamiento de datos personales se realicen conforme a los principios y obligaciones establecidos en esta ley.

j) Relacionarse y colaborar con los órganos públicos en el diseño e implementación de políticas y acciones destinadas a velar por la protección de los datos personales y su correcto tratamiento.

k) Suscribir convenios de cooperación y colaboración con entidades públicas o privadas, nacionales, extranjeras o internacionales, que tengan competencia o estén relacionadas al ámbito de los datos personales. En los casos de suscribir convenios con entidades públicas internacionales se requerirá consultar

previamente al Ministerio de Relaciones Exteriores, de conformidad a lo establecido en el artículo 35 de la ley N° 21.080.

l) Participar, recibir cooperación y colaborar con organismos internacionales en materias de protección de datos personales.

m) Certificar, registrar y supervisar los modelos de prevención de infracciones y los programas de cumplimiento y administrar el Registro Nacional de Cumplimiento y Sanciones.

n) Ejercer las demás funciones y atribuciones que la ley le encomiende."

Sin ánimos de realizar un análisis exhaustivo de las atribuciones que se proponen, pues escaparía los propósitos de este trabajo, cabe destacar que la creación de esta nueva ley, y de un organismo público encargado de resguardar y hacer efectiva la protección de datos personales, se constituye como un esfuerzo para no solo hacerse cargo de los problemas de redacción, interpretación y aplicación de la ley, sino que también de los problemas orgánico-estructurales que nuestro país tiene al carecer de las entidades idóneas a los cuales los titulares puedan acudir para la gestión de la protección de datos.

En las últimas discusiones al respecto de este proyecto de ley se ha propuesto que en caso de que se cree por ley la Agencia de Protección de Datos Personales, esta tenga la característica de ser independiente[47]. Esta propuesta es del todo relevante, pues lo que caracteriza principalmente a una agencia independiente es que se trata de organizaciones de carácter institucional, no representativas, que desarrollan funciones propias de la Administración activa y que están configuradas legalmente de forma que el Gobierno y el resto de la Administración gubernativa carecen de las facultades de dirección que configuran típicamente su relación con la Administración institucional instrumental, con la finalidad de neutralizar políticamente una actividad integrada en la órbita del Poder Ejecutivo[48]. Teniendo en mente que la posibilidad de vulnerar la vida privada puede venir tanto de entes privados como públicos, la noción de independencia es totalmente fundamental en orden de poder resguardar la información sensible de los gobiernos de turno, y que en definitiva todo estos datos estén en manos de un ente técnico que se encuentre alejado del poder político que tenga

[47] *Ibid*. p.7

[48] MAGIDE, M, (2000). Límites constitucionales de las Administraciones independientes. En: CORDERO, L. y GARCIA, J. (2012). Elementos para la discusión sobre agencias independientes en Chile. El caso de las superintendencias. Anuario de Derecho Público, Universidad Diego Portales. Chile. p. 420.

posibilidades de entrometerse con cualquier propósito que ponga en riesgo los principios fundamentales como el de la finalidad.

A su vez, respecto de esta propuesta de Agencia de Protección de Datos en particular, desde la doctrina se ha estimado que la principal novedad de este nuevo organismo administrativo consiste justamente en la creación de una autoridad de control de carácter técnico y una institucionalidad pública que asuma los desafíos regulatorios y de fiscalización en materia de protección de las personas y tratamiento de los datos personales[49]. En consecuencia, esta agencia supone un avance notable en la materia y se articula en torno al objetivo general de que el titular de los datos otorgue su consentimiento y mantenga bajo su control el uso de sus propios datos que efectúe cualquier persona[50]. Si se observa la larga lista de potestades que se busca que esta agencia tenga, y la gran variedad de ámbitos y materias que abarcan (políticas públicas, protección de datos, potestades sancionatorias y coordinación con otros organismos de la Administración del Estado como, por ejemplo, la Contraloría General de la República, entre otras), no existiría inconveniente en afirmar que es una propuesta que da un paso en la dirección correcta para enfrentar de manera holística los problemas asociados a la protección de datos.

Ahora bien, en el contexto de la discusión legislativa del proyecto de ley, y en particular del principio de finalidad, y de los propósitos a los cuales los datos personales de los usuarios deben ser utilizados, el en ese entonces senador Felipe Harboe expresó que:

> *"(…) a pesar de que el mencionado principio se encuentra consagrado por la legislación vigente, la falta de institucionalidad, de acción, de protección real y la evolución tecnológica hace imposible pesquisar la administración y almacenamiento ilícito de datos personales" [51].*

Consecuentemente, se puede apreciar como el principio de finalidad requiere de una estructura institucional que lo vuelva posible, y que le otorgue la efectividad requerida para poder operar en la realidad social y tecnológica que actualmente atraviesa nuestro país, sin mencionar que sea capaz de adecuarse lo mejor posible a los futuros desafíos que se avecinen. Lo cual, como ya se indicó con anterioridad, se facilita importantemente con la

[49] BAUZÁ, F (2019). Op. Cit. p. 124
[50] *Ibid*.
[51]CHILE. Congreso Nacional de Chile. (2017). Informe de la comisión de constitución, legislación, justicia y reglamento recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. p. 62.

creación de la Agencia de protección de datos. En el proyecto de ley, concretamente hablando, este principio se propone que se consagre en los siguientes términos:

> *"Principio de finalidad. Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento de los datos personales debe limitarse al cumplimiento de estos fines.*
>
> *En aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el tratamiento sea para fines compatibles con los autorizados originalmente; exista una relación contractual o pre contractual entre el titular y el responsable que justifique el tratamiento de los datos con una finalidad distinta siempre que se enmarque dentro de los fines del contrato o, sea coherente con las tratativas o negociaciones previas a la celebración del mismo; el titular otorgue nuevamente su consentimiento; los datos provengan de fuentes de acceso público, y cuando lo disponga la ley"* [52].

Del texto citado se pueden advertir fácilmente algunas diferencias a cómo se entiende este principio en la actualidad, pues se hace una especificación muy notable de la finalidad al establecerse causales específicas que muestran la compatibilidad de uso por parte del ente tratante de la información, como por ejemplo las situaciones referentes a relaciones precontractuales. Además, a diferencia del artículo 9 de nuestra Ley de Protección de la Vida Privada vigente, que contempla muchas menos situaciones y no establece deber alguno por parte de la entidad tratante respecto de la compatibilidad, esta nueva norma incluye las exigencias de especificidad, explicitud y licitud, lo cual da cuenta de un seguimiento de la técnica legislativa que se ha dado en las normativas supranacionales más contemporáneas, como la del Reglamento de la Unión Europea en su artículo 5 numero 1.b). Con respecto a este último, si hacemos una lectura profunda de él y de la propuesta de norma que recoge la finalidad que se hace en el proyecto de ley, podemos concluir que se sigue la lógica de la ya mencionada en el capítulo 3, en referencia a la limitación de la finalidad, el cual es un estándar mucho más determinado donde la noción de compatibilidad del uso de datos es fundamental. En resumen, en el proyecto se propone una redacción que permite que el principio de finalidad tenga un ámbito de aplicabilidad muchísimo más claro y determinado, lo que facilitará una protección de los titulares mucho más expedita que la que tenemos hoy.

[52] CHILE. Congreso Nacional de Chile. (2021). Informe de la comisión de hacienda recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletines N° 11.092-07 y 11.144-07, refundidos. p.158.

Finalmente, es relevante mencionar que en el proyecto legislativo, al igual que en la Ley N° 19.628, se ha propuesto un listado de causales respecto de las cuales no se requerirá del consentimiento del titular para poder realizar el tratamiento de datos. Al respecto, se ha propuesto un artículo que disponga lo siguiente:

> *"Artículo 13.- Otras fuentes de licitud del tratamiento de datos. Es lícito el tratamiento de datos personales, sin el consentimiento del titular, en los siguientes casos:*
>
> *a) Cuando los datos han sido recolectados de una fuente de acceso público.*
>
> *b) Cuando el tratamiento esté referido a datos relativos a obligaciones de carácter económico, financiero, bancario o comercial y se realice de conformidad con las normas del Título III de esta ley.*
>
> *c) Cuando el tratamiento sea necesario para la ejecución o el cumplimiento de una obligación legal o lo disponga la ley.*
>
> *d) Cuando el tratamiento de datos sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable, o para la ejecución de medidas precontractuales adoptadas a solicitud del titular.*
>
> *e) Cuando el tratamiento sea necesario para la satisfacción de intereses legítimos del responsable o de un tercero, siempre que con ello no se afecten los derechos y libertades del titular. En todo caso, el titular podrá exigir siempre ser informado sobre el tratamiento que lo afecta y cuál es el interés legítimo en base al cual se efectúa dicho tratamiento.*
>
> *f) Cuando el tratamiento de datos sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia"* [53].

Para efectos de nuestro análisis, resulta llamativo que actualmente la voluntad del legislador se inclina por mantener como causales de excepción el consentimiento del titular para la utilización de datos. Particularmente, es muy relevante ver que los datos de carácter económico, financiero, bancario y comercial continúan siendo una de las excepciones que el proyecto de ley contempla. Esta situación da cuenta de la tensión entre la eficiencia económica y la protección de los titulares de los datos que ya se mencionó someramente con anterioridad

[53] *Ibid*. pp 166-167.

en este texto. Como se esbozó en su momento, el consentimiento y el principio de finalidad son dos elementos que se encuentran estrechamente relacionados al dar cuenta de la autonomía de los individuos y sus decisiones a la hora de gestionar su propia privacidad al desenvolverse en la sociedad. Es por esto que ante este escenario corresponde preguntarse si en este proyecto de ley se pueden identificar mecanismos que puedan subsanar esta separación entre consentimiento y tratamiento de datos, en orden de que el titular tenga la gestión y control de su información suficiente como para poder gestionar adecuadamente su propia información. Respecto de este tema se va a ahondar en la siguiente sección.

En suma, considerando la insuficiencia legislativa que Chile adolece en esta materia, es que podemos afirmar con toda certeza que este proyecto de ley da importantes pasos en la dirección correcta. Esto resulta evidente al constatar la mejor elaboración de estándares de comportamiento esperados en materia de datos personales, lo cual es resultado de utilizar como hoja de ruta los estándares elaborados por la Unión Europea, la OECD, entre otras organizaciones supranacionales. Asimismo, se pueden identificar otras propuestas estructurales referentes a la institucionalidad, como la creación de la Agencia de Protección de Datos, lo cual vuelve posible lograr el objetivo de tener una normativa que esté a la altura de las circunstancias respecto de las necesidades que se han presentado durante los últimos años con los avances tecnológicos en el mundo de la protección de la privacidad.

II. Finalidad, privacidad e intereses económicos en el mercado electrónico, un desafío ante intereses contrapuestos

Como ya se ha indicado a lo largo de esta obra, existen argumentos de carácter económico en la utilización de los datos de las personas en el contexto de negocios electrónicos que ponen en tela de juicio la exigencia de consentimiento en los datos de carácter económico, financiero, bancario o comercial. Esto, a su vez, tiene un profundo impacto en la fisionomía y alcance del principio de finalidad por la estrecha relación que hay entre este y el consentimiento, tal y como ya se ha expuesto. La separación entre consentimiento y uso de los datos se ve manifestada claramente en nuestra legislación vigente, particularmente en el artículo 4 inc. 5 de la Ley N° 19.628, criterio que como ya analizamos, el legislador se inclina por mantener en el proyecto de una nueva Ley de Protección de datos en relación de los datos económicos.

En la discusión parlamentaria, la posición de no constituir un régimen de protección absoluto en este tema ha sido tocada por parte de empresas y organizaciones de la sociedad civil. De este modo, podemos ver cómo Equifax, empresa dedicada al rubro de informes de crédito al consumo, manifiesta mediante sus representantes en la discusión de la nueva ley que, en relación al principio de finalidad, considera como fundamental que exista y que esté claramente definido. Destaca, a su vez, que el enfoque presente en el proyecto de ley pone el énfasis de manera casi exclusiva en la protección de los datos y la propiedad de estos por parte de sus titulares, afectando la generación de nuevas oportunidades y análisis a partir de los mismos datos. Lo anterior, afirmó en su momento, provoca un desincentivo a la actividad económica[54].

Ante este escenario corresponde preguntarse si el proyecto de ley logra equilibrar de algún modo el que no se requiera del consentimiento del titular para el uso de estos datos, y si existe en definitiva algún mecanismo para que las personas puedan hacer valer la limitación de la finalidad para resguardad su personalidad y privacidad. Antes, esta pregunta supone resolver una cuestión previa: ¿Cuál es la función que fundamenta que el consentimiento esté relacionado con el principio de finalidad? La respuesta a esta interrogante se encuentra relacionada con la idea de que el titular posea el control de su propia información, en otras palabras, que la información quede completamente en sus manos. En definitiva, el dar consentimiento para el tratamiento de datos es una manifestación de que la administración de la información de alto interés de una persona queda completamente radicada en su autonomía. Por esta razón, si este requisito de concertación de voluntades no está presente, lo que corresponde es dilucidarse si existen mecanismos para que el titular posea otros medios del control de su información a un nivel adecuado.

La respuesta a esta pregunta se puede encontrar en la creación de la Agencia de Protección de Datos. En este nuevo proyecto de ley se busca dotar a este ente administrativo de diversas potestades fiscalizadoras, e incluso sancionatorias, que permitirían corregir situaciones donde un ente tratante de datos quebrante la finalidad en la utilización de los datos y aún más, disuadir que esta intromisión a la privacidad ocurra ante la posible aplicación de

[54] CHILE. Congreso Nacional de Chile. (2017). Informe de la comisión de constitución, legislación, justicia y reglamento recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. p. 111.

sanciones. Por otro lado, también existe interés de que se manifieste como una instancia a la cual acudir ante cualquier problema con la privacidad que una persona pueda tener.

No obstante todo lo recién mencionado, la mejor potestad que posee esta agencia es que permite que el titular pueda mantener el control de su información y hacer valer la limitación de la finalidad incluso cuando no se exija el consentimiento de este mismo en el contexto de los datos de carácter económico, financiero, bancario o comercial. Esta función se encuentra consagrada en la letra g) del artículo 30 bis propuesto en el proyecto de ley, el cual dispone que la Agencia de Protección de Datos Personales tendrá función y atribución de desarrollar programas, proyectos y acciones de difusión, promoción e información a la ciudadanía, en relación al respeto a la protección de sus datos personales. ¿Por qué resulta tan importante esta función? Porque esto permite mitigar el gran problema de asimetrías de información que usualmente existe entre el titular de los datos y la entidad tratante.

El concepto de asimetría de información es acuñado típicamente como una falla de mercado en el ámbito de la regulación económica. En simples palabras, ocurre que las personas no poseen suficiente información para tomar adecuadamente decisiones a la hora de realizar negocios o adquirir productos y servicios. Esto puede ocurrir, por ejemplo, en los contratos de consumo de determinados mercados[55]. Dicho lo anterior, este fenómeno de insuficiencia o asimetría de información se puede dar en los más diversos ámbitos, como por ejemplo, a la hora de contratar un abogado, ya que en ese mercado profesional la asimetría de información se manifiesta en que quien provee el servicio posee información que el consumidor desconoce y cuyo costo resulta prohibitivo para quien demanda el servicio[56]. En síntesis, cuando el proveedor posee mayor información que el consumidor existen riesgos de ineficiencia, alteración de los precios e incluso de vulneración de los derechos de las personas.

Esta situación también se puede dar con frecuencia en el caso del tratamiento de datos personales, pues el fenómeno del Big Data y los distintos avances tecnológicos dan como resultado la automatización del procedimiento de datos. De este modo, por ejemplo, a la hora de hacer una transacción electrónica donde se requiere información pecuniaria del consumidor, éste puede tomar decisiones sin contar con información suficiente que le permita saber qué pasará con su información y qué medidas se pueden tomar para poder tutelar sus derechos ante alguna vulneración. Justamente con esto se produce la generación de datos sin

[55] Véase BAR-GILL, O. (2012). Seduction by contract. Law, economics, and psychology in consumer markets. Oxford. Oxford University Press.
[56] DE LA MAZA, I. (2004). La tradicional dignidad en la profesión: abogados y publicidad en Chile. Fundación Fernando Fueyo. Universidad Diego Portales. Chile. p. 11

que el titular se percate, produciéndose no solo datos de manera consciente, sino que también de aquellos que se producen con cada movimiento que se realiza en línea de manera inconsciente, y que generalmente están más allá de su control[57]. Por otro lado, estas decisiones automatizadas, en conjunto con la elaboración de perfiles mediante algoritmos que pocas personas conocen o entienden, paradójicamente terminan por excluir al titular[58]. Asimismo, hay que agregar que la generalidad de la población, al no tener formación jurídica, posee poco conocimiento de la regulación normativa de la protección de los datos personales, lo cual se traduce en desconocer de las medidas legales que se pueden tomar para reclamar e intentar subsanar una violación a su privacidad.

Es a propósito de este diagnóstico que resulta absolutamente fundamental implementar el principio de limitación de la finalidad y que no solo se vea acompañado de un nuevo diseño institucional que permita resguardar los derechos de los titulares de mejor modo, sino que también se puedan colmar estas asimetrías de información que la mayoría de las personas presentan y desconocen. Una buena política pública ejercida por esta nueva Agencia de Protección de Datos permitiría que los titulares estén más al tanto de los diferentes procedimientos y protocolos que les faculta para reclamar que se respeten sus derechos, e incluso, que se les indemnicen los daños cuando corresponda. También permitir la posibilidad de que, a la hora de realizar determinadas operaciones por medios digitales, sepan que sus datos de carácter económico serán tratados por algún banco o entidad, y cuáles son las consecuencias que eso trae. Por ejemplo, podría permitir a una sujeto saber qué hacer y qué no hacer si su información personal se encuentra disponibles en una base de datos por endeudamiento. En suma, se logra empoderar la autonomía del titular a la hora de participar en el mercado electrónico y las diferentes situaciones que todo esto trae aparejado. Mientras todo esto ocurre, las empresas y bancos de datos podrán continuar utilizando los datos de las personas ahorrando los costos asociados a tener que solicitar autorizaciones cada vez que se desee realizar algún movimiento.

En conclusión, con esta nueva metodología de regulación de los datos personales hay mucha mayor certeza de las reglas del juego, se logra implementar un claro estándar de limitación de la finalidad (con arreglo a consideraciones de legitimidad), los agentes tratantes podrán hacer el tratamiento de datos de carácter económico, financiero, bancario o comercial de manera expedita, y finalmente se consigue informar y empoderar al titular de los datos en

[57] MILANES, V. (2017) Op. Cit p. 17.
[58] *Ibid*. p. 19.

orden de que puedan utilizar los mecanismos institucionales para proteger y tutelar correctamente sus derechos fundamentales. De este modo, se permitirá encontrar el equilibrio en el correcto funcionamiento del comercio electrónico y la intimidad de las personas.

CONCLUSIONES

A lo largo de este trabajo hemos podido ver cómo en nuestro país tenemos una Ley de Datos Personales que, siendo objeto de diversas críticas apenas entró en vigencia, no ha estado a la altura de las circunstancias respecto a la realidad informática que existe en el mundo el día de hoy, además de encontrarse sin un mecanismo de fiscalización, tutela y sanciones adecuadas como para poder aplicarse a los casos concretos de manera idónea. Por otro lado, se pudo analizar que, si bien han existido modificaciones legislativas en esta materia, en particular referentes de gestión de los datos de carácter económico, financiero, bancario y comercial, estas reformas se han enfocado principalmente en problemas particulares a resolver, tal como era la desviación del uso de datos que se daba en plataformas como DICOM. A mismo tiempo, pudimos ver como en el panorama internacional, los principios, estándares, directrices y normas se han encontrado en constante evolución ante los fenómenos del avance tecnológico, el Big Data, el procesamiento automático de datos, etc. En ese sentido por esto mismo es que se requiere en nuestro país una reforma general que permita el poder hacerse cargo de las problemáticas no solo que se están dando en la actualidad, sino las que nos esperan en el futuro, y que al mismo tiempo pueda encontrar un equilibrio en la protección de las personas y el funcionamiento de la economía digital.

Ante esto pudimos ver que el proyecto de Ley que continúa tramitándose en la actualidad en nuestro parlamento, tiene en consideración muchas de estas situaciones, críticas y desafíos que se han expuesto, en orden de poder entregar una normativa con estándares más precisos, como la limitación de la finalidad, con un nuevo organismo administrativo, como la Agencia de Protección de Datos que responde a un diseño institucional que está a la altura de las circunstancias, con adecuadas potestades para que la privacidad de las personas se vea protegida, y en definitiva con la capacidad de ponderar en equilibrio los intereses de los agentes económicos en el mercado electrónico con los Derechos Fundamentales de los habitantes de nuestro país.

En conclusión, la necesidad de que la tramitación de esta nueva ley de datos personales es más que crucial, ya que la ley que tenemos actualmente simplemente no logra los propósitos que una normativa de estas características debiera perseguir. En este mismo sentido, no sabemos que nos espera en el futuro, la única certeza que se puede afirmar al respecto es que la vida digital llegó para quedarse, y la necesidad de tener normas que protejan nuestra información personal, no solo de carácter pecuniario si no de cualquier índole,

no solo nos permitirá mantener nuestra propia autonomía y personal, sino facilitar la vida en comunidad al interior de la sociedad, hacer que el desarrollo económico sea posible, y vivir una vida segura ante intromisiones de terceros.

BIBLIOGRAFÍA

Bibliografía de autores y autoras:

ALVARADO, F. (2014), “Las fuentes de acceso público a datos personales” Revista Chilena de derecho y tecnología, N°3.Chile pp. 205- 226

BAR- GILL O. (2012). Seduction by contract. Law, economics and psychology in consumer markets. Oxford: Oxford University Press.

BARROS, E. (2010), “Tratado de Responsabilidad Extracontractual.” Santiago, Chile. Editorial Jurídica de Chile.

BAUZÁ, F. (2019). “El modelo europeo de protección de datos. Experiencias para la regulación chilena presente y futura.” Ars Boni et Aequi, N° 15, N° 1, pp. 121-148

BOZZO, S. (2020). “Sobreendeudamiento, sistemas de información crediticia y la protección de los datos personales el consumidor en Chile” Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, segundo semestre del 2020. pp. 99-130.

CORDERO, L. y GARCIA, J. (2012) “Elementos para la discusión sobre agencias independientes en Chile. El caso de las superintendencias” Anuario de Derecho Público, Universidad Diego Portales. Chile. pp. 415-435

CERDA, A. (2012). “Legislación sobre protección de las personas frente al tratamiento de datos personales”. Apuntes de clases, Centro de Estudios en Derecho Informático, Universidad de Chile.

_____ (2011). El “nivel adecuado de protección” para las transferencias internacionales de daros personales desde la unión europea”. Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, primer semestre. pp. 327- 356

DE LA MAZA, I. (2004) “La tradicional dignidad en la profesión: abogados y publicidad en Chile”. Revista Derecho y Humanidades, N°10. Chile

DWORKIN. R. (1984) “Los Derechos en Serio” Editorial Ariel S.A. Barcelona, España.

FERRAJOLI, L. (2000). Garantías, en Jueces para la Democracia, N°38. En CARBONELL, F. y LETELIER R., (2020) Debido proceso y garantías jurisdiccionales. En Curso de Derechos Fundamentales. Editorial Tirant lo Blanch. pp. 345- 378

FIGUEROA, R. (2020). “Derecho de privacidad.” En: Curso de Derechos Fundamentales. Editorial Tirant lo Blanch. pp. 129 – 168

GARRIGA, A. (2016) ”Nuevos retos para la protección de los datos personales en la era del Big Data y de la computación ubicua” Editorial Dykinson , España.

JIJENA, R. (2001) “Sobre la no protección de la intimidad en Chile. Análisis de la Ley 19.628, de Agosto de 1999”. Revista Electrónica de Derecho Informático, N°39. pp. 1-27

_____ (2010) “Actualidad de la protección de datos personales en América latina. El caso de Chile”, Memoria del XIV Congreso Iberoamericano de Derecho e Informática. Monterrey, UANL. México, pp. 413- 431

La privacidad en el sistema legal chileno. (2014) Por Carolina Pincheira “et al”. ONG Derechos Digitales Latinoamérica.

MILANES, V. (2017). “Desafíos en el debate de la protección de datos para Latinoamérica” Transparencia & Sociedad, No. 5, Argentina. pp. 13-31.

SZCZARANSKI, C. (2011). “Un asunto criminal contemporáneo. Rol de las empresas, responsabilidad penal de las personas jurídicas y corrupción”. Editorial jurídica de Chile. Santiago, Chile.

VIAL, F. (2001). “La ley N° 19.628 sobre protección de datos de carácter personal. Una visión general.” Cuadernos de extensión jurídica, Universidad de Los Andes.N°5. Chile. pp. 23- 37

VIAL, V. (2006). “Teoría general del acto jurídico”, 5ta Edición, Editorial Jurídica de Chile. Santiago, Chile

VIOLLIER, P. (2017). “El estado de la protección de datos personales en Chile”, ONG Derechos Digitales Latinoamérica.

ZÚÑIGA, F. (2000). “Criterios para la conciliación entre la libertad de información y el derecho a la vida privada en la jurisprudencia internacional y nacional”, en Revista “Ius et Praxis”, Facultad de Ciencias Jurídicas y Sociales, Universidad de Talca, Año 6 N.º 1. Editorial Universidad de Talca, Talca, Chile. pp. 443- 463

Bibliografía legislativa:

CHILE, Congreso nacional de Chile. Primer trámite en Comisión de Constitución del Senado, que recae en la moción parlamentaria para reforma constitucional que consagra el derecho a la protección de los datos personales. Boletín N° 9.384-07. 2014

CHILE, Congreso Nacional de Chile. Primer trámite de Constitución en el Senado de la Ley N°19.628 sobre datos personales.1999

CHILE, Congreso Nacional de Chile. Primer informe de la comisión de economía, que recae en el proyecto de ley en el segundo tramite constitucional en el Senado que establece el principio de finalidad en datos personales. 2012

CHILE. Congreso Nacional de Chile. Informe de la comisión de constitución, legislación, justicia y reglamento que recae en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletines N° 11.092-07 y 11144- 07. 2017

CHILE. Congreso Nacional de Chile. Informe de la comisión de hacienda recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletines N° 11.092-07 y 11.144-07, refundidos. 2021.

Bibliografía de páginas web:

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Principios. 2021 [en línea] Disponible en: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios

BARRANCO, R. (2012) "¿Qué es el Big Data?" IBM Developer Works . [en línea] Disponible en: https://developer.ibm.com/es/articles/que-es-big-data/

MALDOFF, G. (2016) The Risk-Based Approach in the GDRP: Interpretation and Implications (White Paper). [en línea]
Disponible en: https://iapp.org/resources/article/therisk-based-approach-in-the-gdpr-interpretation-and-implications/

Normativa supranacional:

OCDE. (2013). Directrices sobre la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales.

ONU. (1948). Declaración Universal de los Derechos Humanos

UE. (1981) Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio de Estrasburgo).

UE. (1995). Directiva 95/46/CE de Protección de Datos del Parlamento y Consejo Europeo

UE. (2016). Reglamento General de Protección de Datos de la Unión Europea.