UNIVERSIDAD DE CHILE

Facultad de Derecho

Departamento de Derecho Comercial

AGENCIA DE PROTECCIÓN DE DATOS PERSONALES

MEMORIA PARA OPTAR AL GRADO DE LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

Cristian Alonso Orellana Vilches

Autor

Claudio Magliona Markovicth

Profesor Guía

Santiago de Chile

2021

A mis padres, Cristian y Mary, por su amor y apoyo incondicional.
Por educarme de la forma en que lo han hecho, les estaré eternamente agradecido.
Me esforzaré por hacerlos sentirse orgullosos.

"La democracia se desarrolla y justifica en el respeto de la privacidad de las personas que forman parte de ella, ya que sólo desde el ámbito de reconocimiento de la vida privada y autonomía de cada ciudadano puede construirse una sociedad democrática y libre."

HUMBERTO NOGUEIRA.

TABLA DE CONTENIDO

RESUMEN

La presente memoria se centra en el análisis de la nueva autoridad de control en materia de protección de datos personales en nuestro país, cuya instauración es pretendida en el proyecto de ley modificatorio de la Ley N°19.628 sobre Protección de la vida Privada (Boletín N°11144-07) y que crea la denominada “Agencia de Protección de Datos Personales”.

El análisis de dicho organismo tomará en cuenta, en primer lugar, el desarrollo histórico en la protección de datos personales y la necesidad de otorgar una adecuada protección a este ámbito de la vida privada mediante la dictación de diversas normativas. En segundo lugar, se analizarán las principales críticas que se han realizado a nuestra actual Ley N° 19.628 sobre Protección de la Vida Privada, centrándose, en lo referido a la ausencia de una autoridad de control independiente que resguarde y garantice los derechos de los titulares de datos.

Posteriormente, se realizará un análisis específico de la autoridad de control que se plantea instaurar, haciendo presente las consideraciones y modificaciones que el Proyecto de Ley observó durante su trámite legislativo. El análisis de las características de la autoridad de control nos permitirá observar que su instauración es el camino más adecuado para un efectivo y eficaz resguardo de los derechos de los titulares de datos dentro de nuestro ordenamiento.

Finalmente, se realizará un análisis comparado respecto de una entidad de similares características dentro del ordenamiento español como es la Agencia Española de Protección de Datos, observando las principales similitudes entre ambas autoridades, así como también haciendo presente las oportunidades de mejora que puede observar nuestra pretendida autoridad de control con el fin de poder acercar nuestro ordenamiento jurídico a los estándares internacionales en materia de protección de datos personales.

Palabras Clave: *Datos personales - Agencia de Protección de Datos Personales - autoridad de control - titulares de datos - encargados de datos.*

INTRODUCCIÓN

Desde finales del Siglo XX hemos observado, como sociedad, una revolución tecnológica sin precedentes. Sin duda alguna, los hitos más importantes dicen relación, en lo que ha este trabajo concierne, con la proliferación de nuevas herramientas tecnológicas para facilitar la vida en sociedad (teléfonos inteligentes, computadoras sofisticadas, sistemas de localización, asistentes virtuales, etc.), nuevos medios de comunicación y el nacimiento de mercados *online* que han facilitado la compra por parte de los usuarios, los cuales cuentan hoy con una mayor variedad y accesibilidad de productos y servicios[1].

En la actualidad las ventajas tecnológicas que poseemos respecto de generaciones anteriores, en su gran mayoría, presentan como factor común el uso de Internet para su funcionamiento. Internet ha generado un entramado digital tan poderoso que nos ha permitido cambiar de manera significativa, entre otras cosas, la forma en la que nos comunicamos. Así, por ejemplo, se ha logrado que dos personas de diferentes continentes puedan comunicarse de forma prácticamente inmediata[2], incluso pudiendo observar a la otra persona si es que el dispositivo conectado a internet cuenta con una cámara web.

Ahora, si bien estos fenómenos tecnológicos han traído beneficios para las diversas poblaciones, también cuentan con una cara oculta, respecto de la cual es posible establecer que no hemos reparado con la necesaria detención. La doctrina ha reconocido que el desarrollo de las nuevas tecnologías y, en especial, la informática, han traído aparejado problemáticas nuevas de gran relevancia que han encendido las alertas en torno a la protección de los ámbitos más internos del desarrollo humano[3].

Se ha señalado que "durante la década de 1960 y 1970, el interés por asuntos relativos a la privacidad se incrementó con las nuevas tecnologías de la información. El potencial de las herramientas informáticas para recolectar, procesar y analizar información ponía en peligro la

[1] En torno a esto María Labbé Figueroa sostiene que "los datos pueden ser utilizados como un input en la producción de bienes y servicios al permitir que las empresas productoras de bienes y servicios entreguen productos de mejor calidad a sus clientes, toda vez que mientras más conocimiento tengan las compañías de la valorización que los consumidores dan a las características de los bienes y servicios, tendrán mayores posibilidades de dedicarse a optimizar esos atributos. En consecuencia, los productos puestos a disposición del público serán cada vez más atractivos, debido a que parecerá como si hubiesen sido especialmente creados para satisfacer las necesidades de los consumidores". En: LABBÉ, M. *Big Data:* Nuevos desafíos en materia de libre competencia. *Revista Chilena de Derecho y tecnología,* VOL. 9, Núm. 1, 2020, pp. 33-62. p. 41.

[2] La pandemia del virus Covid-19 ha dejado en evidencia el posicionamiento de Internet como un medio de comunicación esencial, toda vez que ha permitido mantener (en cierto grado óptimo) el funcionamiento de actividades esenciales para la sociedad a través de la comunicación y trabajo a distancia.

[3] QUEZADA, F. La protección de datos personales en la jurisprudencia del tribunal constitucional de Chile. *Revista Chile de Derecho y tecnología,* VOL. 1, Núm. 1, 2012. pp. 125-147. p. 127.

vida privada de los individuos, lo que impulsó las demandas por normas específicas que regularan la recolección y el manejo de información personal. Este avance tecnológico dejó en evidencia que no era suficiente el derecho a la privacidad entendido como el derecho a excluir la injerencia de terceros, sino que se hacía necesario ampliar su protección para que el titular pudiera controlar la información personal que le compete"[4]. Así, "se amplió la concepción de información privada desde un espacio libre de intromisión ajena, a uno donde los titulares de la información pudieran tomar parte en su control, activamente, con la privacidad ya no se aludía a una figura de "espacio reservado" fuera de intromisiones de terceros, sino que a la capacidad del titular de datos de decidir por sí mismo el control del destino de los mismos"[5].

Dicha situación generó la necesidad de establecer mecanismos de control, diferentes en cada Estado, que nos permitieran monitorear y controlar la información que las diversas plataformas web recolectaban de sus usuarios (número telefónico, dirección de correo electrónico, dirección de domicilio, gustos artísticos, preferencias, etc.)[6]; información que las personas entregan a estas plataformas para poder hacer uso de las mismas sin hacer reparo respecto de su posterior utilización o tratamiento. Los usuarios han confiado a las plataformas web información respecto de su propia persona pensando – si es que alguno de los usuarios lo ha hecho – de que dicha información será conservada de manera secreta y que no tendrá un tratamiento posterior[7].

Esta situación ha generado que los datos de las personas se hayan convertido en un bien preciado para entes privados que actúan a través de sitios o páginas web, los cuales se han abocado a la recopilación de estos datos con fines comerciales, obteniéndolos de diversas maneras[8]. En torno este tema se ha sostenido que la información respecto de datos personales "es especialmente valiosa en el mercado y su tratamiento indiscriminado presenta severos riesgos, pues podría permitir conocer o deducir características de la vida de una persona que ella misma preferiría mantener en reserva o lejos del escrutinio público. Los datos recopilados

[4] LARA, J., VERA, F. y SOTO, B. Privacidad y nuevas tecnologías, regulación chilena y propuestas de política pública. *Policy Paper ONG Derechos Digitales,* N°02, 2013. p. 4. [En Línea]: https://www.derechosdigitales.org/wp-content/uploads/pp-02.pdf [consulta: 28- 09- 2021].
[5] LARA, J., VERA, F. y SOTO, B. Ibidem. p.4.
[6] El modelo de negocios de muchas empresas que operan a través de internet comprende la recolección y el análisis de datos, los que se obtienen, principalmente, de quienes acceden a sus plataformas, es decir, de los usuarios de internet que entregan información relevante mientras hacen uso del contenido de las páginas o aplicaciones. En: LABBÉ, M. Op. Cit. p.38
[7] Hoy no debiese ser una sorpresa el saber que Internet ha permitido el almacenamiento de innumerables cantidades de datos, de la más variada índole, sobre cada una de las personas.
[8] A modo de ejemplo se pueden señalar la solicitud de datos para la creación de una cuenta personal en una red social, números de tarjetas bancarias, solicitud de datos para obtener descuentos comerciales, entrega de dirección de domicilio para el envío de un determinado producto adquirido a través de Internet.

en estos sitios adquieren un gran valor para anunciantes y empresas de estudios de mercado en Internet, y por tanto la legislación debe cautelar que el tratamiento de la misma sea respetuoso de la voluntad de sus usuarios, y especialmente de sus derechos fundamentales"[9].

Es importante destacar que no solamente son los privados quienes se han abocado a la tarea de recopilar y tratar los datos de las personas, no es difícil de advertir que los propios Estados se ha visto en la necesidad de recopilar información y datos de sus ciudadanos. Hoy en día el Estado se ha convertido en uno de los principales captadores y procesadores de información personal, información que resulta necesaria, desde un punto de vista estatal, para cumplir eficientemente con la implementación de políticas públicas, la entrega de determinados beneficios o la planificación, gestión y mantención del orden público[10]. Es evidente que para el Estado sería sumamente difícil la realización de las diversas políticas públicas si no se permitiera la obtención de grandes masas de datos de los ciudadanos, considerando siempre que dicha obtención debe obedecer a la misma legalidad que se ven enfrentados los entes privados; no es posible sostener que el Estado debe verse ajeno a la legislación en materia de protección de datos personales, una afirmación en tal sentido significaría permitir una directa afectación a los derechos fundamentales de las personas.

A raíz de lo señalado, en las últimas décadas los Estados han tomado la decisión de generar cuerpos normativos que regulen la recopilación y tratamiento de los datos personales, con el fin de poder salvaguardar la privacidad de las personas y, más importante aún, impedir la realización de conductas que puedan atentar contra los derechos fundamentales de los individuos. Estas diversas legislaciones han adoptado no solo normativa aplicable a la recopilación y tratamiento, sino que además han optado (en muchos casos) por la creación de órganos públicos independientes y especializados que se abocan a la fiscalización y conocimiento de los problemas que se susciten con motivo del tratamiento de datos personales. Además, se ha dotado a dichos organismos con facultades sancionatorias frente a situaciones que infrinjan la normativa correspondiente.

Cabe hacer presente en este punto que nuestro país, lamentablemente, no ha ido a la par de otros ordenamientos en la dictación de nuevas regulaciones en materia de datos personales. Nuestra legislación ha devenido en obsoleta y poco eficiente para proteger a las personas frente a actos que signifiquen un tratamiento indebido de sus datos. La referida

[9] LARA, J., VERA, F. y SOTO, B. Op. Cit. p. 6.
[10] MATUS, J. Derecho de acceso a la información pública y protección de datos personales. *Revista Chilena de Derecho y Tecnología*, VOL. 2 Núm. 1, 2013, pp. 197-228, p. 199.

obsolescencia de nuestra legislación se fundamenta en el hecho de que nuestra principal normativa en materia de protección de datos personales, la Ley N° 19.628 sobre Protección de la Vida Privada (en adelante la "La Ley" o "Ley N° 19.628"), data del año 1999, fecha desde la cual ha recibido pocas, y no tan eficaces, modificaciones que nos permitan ajustar nuestra legislación a los estándares internacionales.

En una crítica realizada por distintas ONGs nacionales, se dejó en evidencia que "Chile sufre de una paradoja: Reconoce estándares de protección de la privacidad basados en su Constitución, así como en tratados internacionales de derechos humanos, pero su ley interna es absolutamente deficiente para garantizar dicha protección. Existe consenso entre los expertos en que la LPD (Ley N° 19.628) que regula la materia resulta deficitaria por distintas razones: i) la ausencia de sanciones efectivas, ii) falta de una regulación de flujo transfronterizo de datos, iii) falta de un registro de banco de datos privados, iv) ausencia de una autoridad pública de control, v) amplias excepciones al consentimiento en el tratamiento de datos, y vi) falta de mecanismos procedimentales de resguardo efectivo de los derechos reconocidos en la ley. Como consecuencia, en la práctica la ley ha servido más para legitimar el tratamiento indiscriminado de datos personales, que para proteger a las personas"[11].

Es por lo anterior que en este trabajo se realizará un análisis respecto a la situación actual de nuestro ordenamiento jurídico en materia de protección de datos personales, analizando la legislación y los mecanismos que se han adoptado para la protección de los derechos de los titulares de datos. Este análisis dará paso a la revisión del último gran proyecto modificatorio de la Ley N° 19.628 presentado ante nuestro Congreso, contenido en el Boletín N° 11.144-07[12], el cual pretende actualizar y mejorar nuestra legislación en materia de datos personales.

Si bien el proyecto modificatorio presenta varias cuestiones interesantes, que pueden ser materia de posteriores análisis, en este trabajo el foco estará puesto sobre la nueva entidad fiscalizadora en materia de datos personales que se consagra, la denominada "Agencia de Protección de Datos Personales". Se analizará cómo esta entidad, que aparece como un órgano autónomo y especializado, logrará acercarnos a los estándares internacionales y nos

[11] COMUNICACIÓN CONJUNTA DE DERECHOS DIGITALES, CIUDADANO INTELIGENTE, FUNDACIÓN PRO ACCESO, Y PRIVACY INTERNATIONAL. El derecho a la privacidad, 2019. p. 9. [En Línea]: https://www.derechosdigitales.org/wp-content/uploads/EPU-Chile_Privacidad_Presentado-1.pdf [Consulta: 29-09-2021]

[12] Proyecto que a la fecha de elaboración de este trabajo se encuentra en primer trámite constitucional.

permitirá entregar una protección eficaz a las personas sobre sus datos personales, de cara a las actuaciones intromisivas llevadas a cabo por parte de entes privados o de parte del Estado.

En dicho análisis, resultará fundamental, la enunciación, comprensión y análisis de las características de la nueva Agencia de Protección de Datos Personales, así como también el conocimiento de las implicancias que trae la instauración de un órgano público especializado como el que se pretende en nuestro sistema.

CAPÍTULO I: PROTECCIÓN DE DATOS PERSONALES

Tal como se señaló en la introducción del presente trabajo, a raíz de los avances tecnológicos y la proliferación de Internet, se hizo necesario que los diversos Estados fueran adoptando normativas, de diversas indoles, que permitieran controlar las nuevas (y numerosas) situaciones que se generaban. Las diversas posiciones ideológicas y doctrinarias comenzaron a marcar puntos de unión en torno a la idea de que las nuevas sociedades, desarrolladas al alero de las nuevas tecnologías, conllevarían insospechadas posibilidades de reunir, almacenar, relacionar y transmitir todo tipo de información que bien los poderes públicos, bien los sujetos privados, utilizarían para tener conocimiento de amplias parcelas de nuestras vidas y hacer uso de dicha información para su beneficio[13].

Particularmente, uno de los temas más relevantes que hizo eco en los diversos Estados decía relación con la información que, de manera masiva, comenzaba a circular por la red. La creciente utilización de tecnologías informáticas y digitales por parte de órganos del Estado, del sector privado y de la propia ciudadanía para la captura, procesamiento y transmisión de información personal, levantó varias alarmas respecto del impacto que este tipo de herramientas podía tener en la protección de los derechos fundamentales de las personas[14]. Esto se convirtió en un tema relevante debido a que hasta la irrupción de internet prácticamente la única forma en que la información relevante de una persona llegaba a manos de algún ente privado era mediante la entrega de dichos datos de forma voluntaria (y presencial en muchos casos) por parte del titular[15].

De esta forma, el devenir de las nuevas tecnologías parecía dejar atrás parcelas de privacidad que habían permanecido a resguardo. Ante esto se comenzó a gestar en Estados Unidos, a fines de la década de los sesenta, una doctrina (encabezada por los profesores Westin y Fried) que contribuyó a "extender la privacidad desde una noción pasiva, centrada en la simple retención de información –esto es, la ausencia de información sobre nosotros en las mentes de otros, o, si se prefiere, reivindicación de un espacio exclusivo y excluyente– a

[13] QUEZADA, F. Op. cit. p. 126.
[14] ÁLVAREZ, D. La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa. *Revista Chilena de Derecho y Tecnología,* VOL. 9 N°1, 2020, pp. 1-4. p.1.
[15] Respecto del Estado la información siempre ha sido captada de forma conjunta por las distintas instituciones públicas, las cuales actúan en colaboración para poder dar aplicación a las políticas públicas con mayor facilidad.

una activa, que releva el control y disposición sobre cuándo, quién y para qué puede acceder a la información que nos concierne"[16].

Esta idea de privacidad o esferas de privacidad, como contraposición a la obtención de información por parte de terceros, dio origen a la concepción de un derecho que la doctrina denominó "Autodeterminación Informativa". Este derecho se tradujo en el control de las personas sobre sus datos, comprendiendo "el derecho a saber sobre la existencia de ficheros o archivos de registro de información de carácter personal, públicos o privados, cuáles son sus finalidades y quiénes son los responsables de los mismos, de manera que las personas concernidas puedan conocer los datos propios contenidos en dichos archivos o ficheros, teniendo el derecho a actualizarlos o a solicitar mediante el recurso de habeas data su rectificación o cancelación"[17].

En un mismo orden de cosas, la doctrina comenzó a plantearse la discusión en torno a si la protección frente al tratamiento de los datos personales constituía "la expresión de un derecho ya existente, cual es el derecho a la intimidad, o bien representa una nueva categoría de derecho, que garantiza a las personas facultades de información, acceso y control de los datos que le conciernen, prescindiendo de si por su propia naturaleza el tratamiento de tales datos constituye una lesión a la intimidad de las personas a quienes se refieren"[18].

Dicha discusión no resultó ajena a nuestro ordenamiento jurídico, cuestión que se evidencia en el hecho de que nuestro Excelentísimo Tribunal Constitucional ha debido manifestarse al respecto. Así, nuestro Excelentísimo Tribunal Constitucional sentenció que:

"*la protección de la vida privada de las personas guarda una estrecha relación con la protección de los datos personales, configurando lo que la doctrina llama derecho a la autodeterminación informativa. […] Ello se traduce en el control de las personas sobre sus datos y comprende el derecho a saber sobre la existencia de ficheros o archivos de registro de información de carácter personal, públicos o privados, cuáles son sus finalidades y quiénes son los responsables de los mismos, de manera que las personas concernidas puedan*

[16] CERDA, A. Autodeterminación Informativa y Leyes Sobre Protección de Datos. *Revista Chilena de Derecho Informático,* Núm. 3, 2003. pp. 47- 75. p. 50.
[17] QUEZADA, F. Op. Cit. p. 138.
[18] CERDA, A. Op. Cit. pp. 52-53.

conocer los datos propios contenidos en dichos archivos o ficheros, teniendo el derecho a actualizarlos o a solicitar mediante el recurso de habeas data su rectificación o cancelación"[19].

A pesar de lo antes señalado, hoy la discusión se ha zanjado en torno a la idea de que constituyen dos derechos diferentes, donde por un lado tenemos el derecho (y respeto) a la vida privada e intimidad y, por otro, el derecho de protección sobre los datos personales, los cuales en ciertos casos tendrán la calidad de datos relacionados con cuestiones privadas. Así, la doctrina ha señalado que "la protección de los datos personales nace como una derivación del derecho a la privacidad que llega incluso a configurar un nuevo derecho fundamental, reconocido ya en 1983 en la famosa sentencia del tribunal constitucional alemán en el caso de la Ley de Censo de Población: el derecho a la autodeterminación informativa. Este derecho confiere a su titular un haz de facultades para controlar la información que respecto de los datos personales que le conciernen puedan ser albergados, procesados o suministrados informáticamente, variando desde el concepto tradicional que manifestaba una faz negativa del derecho"[20].

Por su parte, el Tribunal Constitucional Español ha señalado que "la protección de datos personales es un derecho distinto de la intimidad, tanto en su función como en su objeto y contenido. En materia de función, mientras que la intimidad protege frente invasiones al "ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad", la protección de datos personales tiene por función garantizar a su titular "un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado". Por ello, el objetivo del derecho a la protección de datos personales es más amplio que el de la intimidad"[21].

Con lo expuesto podemos establecer que, en resumen, la doctrina nos ha señalado a lo largo de estos años que "el tratamiento de datos personales debe reconocer su fundamento en la protección y tutela de la autodeterminación informativa o, como también se le conoce, en el derecho fundamental a la protección de datos personales. A diferencia de lo que pudiere pensarse, el derecho de autodeterminación informativa no es un impedimento al tratamiento de datos personales, sino que, jurídicamente, da el sustento a dichos tratamientos. Este

[19] TRIBUNAL CONSITUCIONAL, Roles N° 1732-10 y 1800-10, de 21 de junio de 2011, cons. 25°." En: CONTRERAS, P. El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la constitución chilena. *Estudios Constitucionales,* vol. 18, núm. 2, 2020. pp. 87-120. p.95.
[20] LARA, J., VERA, F. y SOTO, B. Op. Cit. p. 4.
[21]CONTRERAS, P. Op. Cit. p.91

derecho supone el autocontrol y la autonomía de decisión del individuo, titular del derecho, respecto de su información personal e impone un mandato al legislador y a todos los órganos del Estado de protección de los datos personales"[22].

I.1.- NECESIDAD DE REGULACIÓN

El caudal de información nominativa susceptible de ser tratada por medios informáticos y aún transmitida a distancia gracias al desarrollo de las telecomunicaciones, despertó la precaución de quienes veían en ello un serio riesgo para los derechos fundamentales, debido a se permite a quien dispone de la información acceder a parcelas de nuestra vida que legítimamente debían tenerse a su resguardo y aun servirse de ella para condicionar el ejercicio de nuestras libertades[23].

En la misma línea sostuvo el profesor Alberto Cerda que "si los medios de comunicación de masas importaban un serio riesgo para la intimidad, las nuevas tecnologías lo son aún más, desde que han generado una insospechada capacidad para recoger, procesar y transmitir información; en efecto, el progresivo incremento en el empleo de la informática por servicios públicos y particulares, ha permitido a estos disponer de más y mejor información, conforme a la cual adoptar las decisiones atinentes a sus ámbitos de competencia: así, por ejemplo, en unos casos se tratará de concesión de subsidios o beneficios, en otros el propósito será prever el comportamiento del mercado ante la introducción de un nuevo bien o servicio"[24].

Así, a raíz de la proliferación de caudales masivos de información, los Estados se vieron en la necesidad de crear normativas en favor de la protección de aquellos datos que eran recopilados de forma masiva, debido a las posibles afectaciones de derechos que se pudieran generar. Esta idea es recogida por don Humberto Nogueira, quien sostiene que "el conjunto de servicios de naturaleza informática que pueden ser prestados a través de una red de comunicaciones, presenta, junto con el progreso y sus aportes al desarrollo de las sociedades, riesgos importantes para el respeto de la vida privada e intimidad de las personas, por su capacidad de reunir datos, interrelacionarlos, ordenarlos, posibilitando el acceso a ellos y a transmitirlos, de manera de constituir importantes bases de datos con información de las

[22] CONTRERAS, P., TRIGO, P. Interés legítimo y tratamiento de datos personales: antecedentes comparados y regulación en Chile. *Revista de Derecho y Tecnología,* VOL. 8, Núm.1, 2019, pp. 69-196. p.71.
[23] CERDA, A. Op. Cit. p. 51.
[24] CERDA, A. Op. Cit. p. 50.

personas tanto en manos del Estado como de particulares, con desconocimiento de los afectados.

El registro, procesamiento, entrecruzamiento, organización y transmisión de datos constituye una información valiosa para todo tipo de toma de decisiones económicas, políticas, sociales, empresariales; las bases o registros de datos personales implican la posibilidad de develar aspectos de la vida privada de las personas, haciendo ilusorio su derecho a la privacidad, lo que exige su regulación por el ordenamiento jurídico"[25].

Esta preocupación dio origen a una serie de normativas internacionales cuyo motivo principal decía relación con la protección de los datos personales y los derechos que sobre estos poseen los particulares o titulares de datos. Ejemplos de estas normativas son el Convenio 108 adoptado por la Comunidad Económica Europea (1981); la "Recomendación relativa a las directrices aplicables a la protección de la vida privada y a los flujos transfronteras de datos personales" de la OCDE (1980); la Convención Americana de Derechos Humanos (1969)[26]; la Carta de Derechos Fundamentales de la Unión Europea (2000); el Reglamento 2016/679 de la Unión Europea (2016)[27].

Con estas normativas lo que se ha intentado es encontrar un equilibrio global que armonice la obtención de información relevante con la debida protección de la esfera privada de las personas. Es decir, "los Estados se han preocupado de determinar los límites legítimos dentro de los cuales puede concretarse la actividad de obtención, tratamiento y difusión o comunicación de datos personales y el derecho de acceso a la información pública que forma parte del derecho a la libertad de buscar y difundir información. Se trata, por tanto, de conjugar armónicamente los derechos a la libertad de buscar y difundir información y el derecho al respeto de la vida privada en el contexto de la informativa y la telemática"[28].

Es claro que este objetivo no es fácil en una sociedad informática como en la que vivimos y, por lo tanto, es misión de cada Estado encontrar "una hoja de ruta que tome como referencia las principales aportaciones que, desde una perspectiva internacional, se han desarrollado en torno a la protección de datos personales y en su relación con el derecho a la

[25] NOGUEIRA, H. Autodeterminación informativa y hábeas data en Chile e información comparativa. *Anuario de Derecho Constitucional Latinoamericano*, Universidad Nacional Autónoma de México, Tomo II, 2005, pp. 449-471. p. 449. [En Línea]: https://revistas-colaboracion.juridicas.unam.mx/index.php/anuario-derecho-constitucional/article/view/30267/27321 [consulta: 12 Octubre 2021].
[26] En lo tocante a su art. 7 sobre los derechos de privacidad y honra.
[27] Es importante destacar también, dentro del marco de nuestro continente, el "Informe jurídico interamericano (CJI)" de fecha 8 de Abril de 2021 de la OEA que consagró los principios actualizados del comité jurídico interamericano sobre la privacidad y la protección de datos personales.
[28] NOGUEIRA, H. Op. Cit. p. 450.

vida privada, con el objeto de establecer aquellos parámetros que sirvan de guía para dar un próximo paso en el fortalecimiento de la protección de la persona respecto del tratamiento de su información y, con ello, evitar injerencias indebidas, sea del sector privado o, más grave aún, del sector público, que incidan en una vulneración de su privacidad"[29].

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

En busca de una hoja de ruta en la protección de datos personales, nuestro país también ha tomado una serie de decisiones relevantes, por ejemplo, "ha suscrito y ratificado diversas convenciones y tratados internacionales, que se refieren a la protección de la privacidad y de datos personales. Ratificó el Pacto Internacional de Derechos Civiles y Políticos, cuyo artículo 17 protege la privacidad. Desde el 8 de octubre de 1990, Chile es signatario de la Convención Americana sobre Derechos Humanos, que en su artículo 11 también garantiza la privacidad. A todos los tratados de derechos humanos ratificados por Chile se les han concedido la misma jerarquía legal que la Constitución Política de acuerdo con el artículo quinto de la misma"[30].

Pero, no solo se ha optado por la suscripción de normativa internacional, sino que ha optado por la dictación de una normativa especializada en materia de datos personales que regula el tratamiento de información de las personas, establece ciertos derechos y deberes para el tratamiento y captación de datos, y crea un mecanismo judicial de indemnización en los casos de vulneración.

De esta forma, el legislador dio origen a la Ley N°19.628 de 1999 sobre Protección de la Vida Privada, la cual, según consta en la historia de la Ley, venía a llenar un vacío manifiesto en nuestro ordenamiento jurídico, teniendo como propósito dar una adecuada protección al derecho a la privacidad de las personas ante eventuales intromisiones ilegítimas, sin distinción respecto a la naturaleza jurídica de quien realizara la intromisión[31]. Nuestro país se configuró como un sistema jurídico particular en el ámbito sudamericano al establecer una ley y procedimiento judicial específico para la protección de datos personales; en el ámbito

[29] MAQUEO, M., MORENO, J., RECIO, M. Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de Derecho,* Vol. XXX, N°1, 2017, pp. 77-96. p.79.
[30] COMUNICACIÓN CONJUNTA DE DERECHOS DIGITALES, CIUDADANO INTELIGENTE, FUNDACIÓN PRO ACCESO, Y PRIVACY INTERNATIONAL. Op. Cit. p. 1.
[31]Historia de la Ley N°19.628, Biblioteca Congreso Nacional. p. 3. [En línea]: https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/6814/ [Consulta: 28 junio de 2021].

sudamericano la regla general había sido establecer, para la defensa del derecho a la autodeterminación informativa y la protección de datos la creación de medios procesales específicos, donde se utilizó la acción de *habeas data* o el recurso de amparo o tutela como medios procesales idóneos[32].

Esta nueva Ley sobre protección de datos personales venía a ser la bajada legal de los derechos fundamentales consagrados en el artículo 19 N°4 de nuestra Constitución, artículo el cual mencionaba como dignos de protección y respeto "la vida privada y la honra de la persona y su familia".

La Ley, además, venía a dar cumplimiento a lo que otros países ya habían realizado en la materia[33], entregando a nuestro ordenamiento jurídico un nuevo estándar en la protección de los datos de la vida privada de las personas y, en particular, consagrando el derecho a la "autodeterminación informativa". Derecho que, como se señaló con anterioridad, ha sido entendido en "términos simples como el "control que ofrece a las personas sobre el uso por terceros de información sobre ellas mismas". El rasgo de autodeterminación como autocontrol es expresión de su fundamento: el libre desarrollo de la personalidad. Normativamente, garantizar una autonomía decisional respecto de la información personal de un individuo es lo que posibilita el libre desarrollo de la personalidad"[34].

Este derecho "obliga al Estado a tratar a los miembros de la comunidad política como personas capaces de autodeterminarse, entre otras cosas, en el uso de su información personal, con el objeto de que puedan programar su propio plan de vida. En otros términos,

---

[32] NOGUEIRA, H. Op. Cit. p. 455.
Nogueira además sostiene que "en el constitucionalismo sudamericano, diversas Cartas Fundamentales de las última décadas del siglo CC incorporan en sus ordenamientos el derecho a la autodeterminación informativa o libertad informática y la institución del hábeas data ; tal es el caso de Brasil, Colombia, Paraguay, Perú, Argentina, Ecuador, Venezuela. En tales Constituciones el hábeas data es regulado junto con las acciones de hábeas corpus y de amparo o tutela, como garantías jurisdiccionales protectoras de la vida privada, intimidad, imagen y honra o buen nombre de las personas".

[33] Las primeras leyes sobre protección de las personas frente al tratamiento automatizado de sus datos se remontan a la primera mitad de la década de los setenta; Cabe mencionar como primera ley en la materia la *Datenschutz,* ley sobre tratamiento de datos personales del Land de Hesse, en la República Federal de Alemania en 1970.
Ley que creó la figura del Comisionario de Protección de Datos, el cual garantizaba independencia para el desempeño de sus funciones, cuales eran velar por la observancia de los preceptos de la propia ley y cuantos otros hicieren referencia al trato de los datos de los ciudadanos.
Otros ejemplos vienen dados por la Data Lag 1973/289 en Suecia; la *Privacy Act* de 1974 en Estados Unidos; la Ley relativa a la Informática y Libertades de 1798 en Francia (*Loi n° 78-17).*
Hoy, todos los Estados miembros de la Unión europea disponen de ellas, y son varios los Estados americanos que también las han adoptado. Es un fenómeno que se ha esparcido por todo el mundo a la luz de la capacidad de almacenamiento y tratamiento de información que posee el equipamiento informático actual. En: CERDA, A. Op. Cit. pp. 56-59.

[34] CONTRERAS, P. El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la constitución chilena. Op. Cit. p.100.

tratarlas como fines en sí mismos. Por ello, la autodeterminación informativa garantizaría "la facultad del individuo de decidir básicamente por sí sólo sobre la difusión y utilización de sus datos personales". Esto impide la instrumentalización de las personas y reducirlas a meros medios para alcanzar fines privados o estatales"[35].

Ahora, si bien la normativa en la época de su dictación fue una gran avance en la protección de los datos personales[36], hoy en día ha devenido en una ley anticuada que no es capaz de cumplir el fin que la motivó, es decir, no brinda el amparo adecuado al bien jurídico que pretende proteger[37]. Se ha observado que el uso protector de la Ley "ha sido prácticamente nulo, orientándose en legalizar el mercado de datos personales en Chile, más ya que sus normas carecen de herramientas efectivas de control tales como un ente regulador y fiscalizador, procedimientos de acceso y ejercicio de otros derechos concordantes con el entorno tecnológico"[38].

Lo anterior debe ser tomado con la debida importancia, ya que las normativas sobre protección de datos personales no solo deben pretender resguardar la intimidad de las personas, sino que además deben resguardar la autodeterminación informática, bajo cuyo alero se confiere a los titulares de datos facultades para controlar la información que el Estado o los privados puedan tener sobre su persona, sin importar si esta información alude o no a circunstancias de su vida privada[39]; esta función hoy no se observa como cumplida bajo el actual sistema de protección de datos personales imperante en nuestro país.

Las falencias de nuestra legislación han sido evidenciadas por nuestra doctrina en diversos ámbitos de la misma, señalándose como ejemplos el hecho de carecer de un catálogo

---

[35] CONTRERAS, P. Idem. p. 101.

[36] La primera en Sudamérica en tratar la materia.

[37] Según la encuesta de *Unisys Index* sobre la percepción de seguridad en Chile, el 73% de los ciudadanos chilenos están seriamente preocupados por la seguridad de sus datos cuando hace compras *on line*, un 76% se encuentra preocupado por la posibilidad que le roben sus datos financieros y un 14% admite haber sufrido un robo de datos personales cuando ha utilizado sitios de comercio electrónico. Por su parte, en el XI Estudio Nacional de Transparencia y Protección de Datos Personales (2019) del Consejo para la Transparencia, a un 41% de los chilenos les preocupa poder ser víctima de delincuencia digital (robo, estafa, chantaje, hackeo, fraude, suplantación de identidad). Según la encuesta de IPSOS para Microsoft36 sobre la Ciberseguridad en Chile, de las 202 empresas incluidas, un 39% admitió haber sufrido ataques por parte de piratas informáticos. De estos, un 17% sufrió la alteración de los datos y el 44% la pérdida del acceso al archivo de datos. Esto se debe, en parte, a la falta de una regulación fuerte que establezca reglas claras que las empresas deben cumplir a la hora de almacenar y procesar datos personales y a la ausencia de una agencia responsable de la protección de los datos personales que pueda actuar como controlador y fiscalizador de las empresas privadas y públicas. En: CONSEJO PARA LA TRANSPARENCIA. Protección de Datos Personales en la era de la economía digital. *Cuaderno de trabajo N°15,* , 2020, p. 20 [En Línea]: https://www.consejotransparencia.cl/wp-content/uploads/estudios/2020/10/Economi%CC%81a-digital-V4.pdf [Consulta: 29 Octubre 2021].

[38] GARRIDO, R. La seguridad en el tratamiento de datos personales. *Ciudadanas 2020 III, El Gobierno de la Información,* Instituto Chileno de Derecho y Tecnologías, 2015, pp. 77- 92. p.79.

[39] CERDA, A. Op. cit. p.73.

detallado y exhaustivo de derechos en torno a la protección de las diversas categorías de datos personales; el uso de términos poco actualizados tales como “banco de datos”[40]; la falta de sanciones e infracciones claras y efectivas; la inexistencia de una autoridad de control especializada y la falta de establecimiento de un procedimiento mediante el cual se pueda hacer efectiva la protección de los derechos consagrados en la misma.

En torno a esto, es importante destacar que as críticas a la legislación no es cuestión baladí, toda vez que dichos factores son fundamentales en la concepción de un sistema de protección de datos personales eficaz. Las observaciones realizadas por la doctrina nos permiten indicar que nuestro sistema no ha resultado idóneo en la protección de los derechos de los titulares de datos, así como tampoco hemos logrado acercarnos a los estándares internacionales imperantes en la materia. A raíz de esto es que resulta relevante analizar ciertas situaciones de relevancia que nos permiten comprender el por qué de la falta de aplicación práctica de la normativa que contiene la Ley N°19.628, así como también comprender los cuestionamiento que ha realizado la doctrina nacional.

II.1.- MECANISMOS DE PROTECCIÓN DE DATOS PERSONALES BAJO LA ACTUAL NORMATIVA

Un primer punto, que reviste importancia respecto de las críticas a nuestra legislación en la materia, y que posee estrecha relación con el tema central de este trabajo, es la falta de un procedimiento especializado de reclamación ante la vulneración de los derechos emanados de la Ley.

La ausencia de un procedimiento especializado de reclamación, dentro de un sistema organizado bajo el amparo de un órgano de control especializado, ha provocado que la protección de los derechos (en materia de datos personales) se haya realizado, en la práctica, a través de dos mecanismos diferentes como lo es, en primer lugar, el denominado *Habeas data (*consagrado en el artículo 12 de la Ley N°19.628) y, en segundo lugar, el recurso de protección en base al numeral 4 del artículo 19 de nuestra Constitución Política de la República; dicha normativa ha sido utilizada como marco jurídico general para resolver cuestiones en torno al tratamiento y protección de los datos personales dentro de nuestro país.

[40] Término que hoy deviene en insuficiente y anticuado, toda vez que hoy los datos personales de las personas no se encuentran propia y exclusivamente en “bancos de datos”, sino que pueden encontrarse en contenedores de diversa índole, por ejemplo, publicados en algún foro, página web o una aplicación de red social.

Esta situación muestra que "si bien la ley reconoce una serie de derechos a las personas naturales titulares de los datos, estos deben ser ejercidos ante tribunales civiles, en procedimiento de larga y costosa tramitación, lo que constituye una barrera para el ciudadano común"[41]. Pudiendo sostenerse, además, que "el sistema de protección de datos personales que tenemos en Chile es reactivo, únicamente dirime los conflictos que el particular afectado promueve, en teoría, ante los tribunales ordinarios, y, en la práctica, por la vía de la acción constitucional de protección; no contamos con un sistema que promueva, proteja y promocione los derechos consagrados en la Constitución y en la LPVP, mediante la realización de acciones positivas tales como campañas de educación y difusión de estos derechos, por ejemplo"[42].

Por tanto, resulta relevante estudiar cómo se ha llevado a cabo la protección de datos personales dentro de nuestro ordenamiento a través de los mecanismos señalados con anterioridad.

II.2.1.- Hábeas Data

En primer lugar, se debe señalar que la expresión Hábeas Data "literalmente significa 'tengas los datos' y su objeto es asegurar el acceso a la información que de la persona afectada tengan registros o bancos de datos públicos o privados, con el objeto de proteger la vida privada, intimidad, imagen, buena reputación u honra de las personas.

El Hábeas Data constituye una acción jurisdiccional protectora de la libertad informática o derecho de autodeterminación informativa (conocimiento y control de datos referidos a la persona) y protección de la vida privada, imagen, honra o reputación de la persona, frente a la recolección, transmisión y publicidad de información que forma parte de la vida privada o intimidad de la persona desarrollada por registros o bancos de datos públicos o privados"[43].

[41] ÁLVAREZ, D. Acceso a la información pública y protección de datos personales: ¿puede el consejo para la transparencia ser la autoridad de control en materia de protección de datos?. *Revista de derecho (Coquimbo)*, *23*(1), 2016, pp. 51-79. p. 53. [En Línea]: https://dx.doi.org/10.4067/S0718-97532016000100003 [consulta: 28 julio 2021].
[42] ÁLVAREZ, D. Ídem. p. 65.
[43] NOGUEIRA, H. Op. Cit. p. 458.

A raíz de la lectura de nuestra Ley N° 19.628 podemos señalar que el artículo 12 de dicho cuerpo normativo, ubicado dentro del Título II sobre "De los derechos de los titulares de datos", consagra este llamado derecho de acceso, *Hábeas Data o Hábeas Scriptum*[44].

Así, nuestra legislación ha establecido el Hábeas Data como "un derecho de rango legal y procesal que vino a desarrollar la garantía o el derecho público subjetivo del respeto (por la sociedad toda) y de la protección (por el ordenamiento jurídico) de la vida privada de la persona y su familia, que contempla y asegura para todas las personas el artículo 19 número 4 de la Constitución Política.

Por su intermedio cada titular puede requerir a quien sea el responsable de una base o banco de datos nominativos en un servicio público, conocer y corregir, modificar o actualizar la información computacional, tratándose de datos personales, nominativos, o relativos a cualquier información concerniente a personas naturales, identificadas o identificables, particularmente si son antecedentes sensibles o referidos a características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como —dice la ley— sus hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual"[45].

Por su parte, el artículo 16 de la Ley N° 19.628 establece un procedimiento especial, cuya conocimiento es de competencia de los tribunales ordinarios, a través del cual los titulares

---

[44] Artículo 12.- *Toda persona tiene derecho a 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.*

En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen.

Sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos.

Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

En el caso de los incisos anteriores, la información, modificación o eliminación de los datos serán absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que haya transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita sólo podrá ejercerse personalmente.

Si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada. Si no fuese posible determinar las personas a quienes se les hayan comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos.

[45] JIJENA, R. Tratamiento de datos personales en el Estado y acceso a la información pública. *Revista Chilena de Derecho y Tecnología*, Vol. 2 Núm. 2, 2013, pp. 49-94, p.62

de datos que resulten afectados pueden ejercer el derecho consagrado en el art.12 del mismo cuerpo legal.

Sin entrar en detalles respecto de esta acción, cabe mencionar que es posible de ser ejercida por todos los titulares de datos que, observando sobre sus derechos, pretendan ejercer las garantías de acceso, rectificación, cancelación u oposición consagradas en la ley[46]. Por su parte, se debe sostener que los sujetos pasivos de dicha acción serán aquellas personas (jurídicas o naturales) a cargo de los bancos de datos; en el caso de órganos de la administración pública el responsable será el o los organismos respectivos que se encuentren a cargo del banco de datos.

Además, esta acción " puede tener un carácter preventivo o correctivo. En su dimensión preventiva tiene por objeto conocer la existencia de registros o bancos de datos que contengan informaciones de las que sea titular y acceder a ellas. La acción en su dimensión correctiva consiste en exigir que determinados datos personales del titular sean corregidos, rectificados, cancelados o bloqueados, por el hecho de que su tratamiento es ilegal y conculca derechos fundamentales"[47].

Una mirada rápida en torno a la consagración del Hábeas Data dentro de nuestra legislación nos podría hacer pensar que los datos personales se encuentran debidamente protegidos, pero esto no es efectivo. El procedimiento consagrado en el art.16 de la Ley N° 19.628 ha tenido escaza aplicación práctica debido, en gran parte, a que debe ser ejercida por el titular ante los tribunales ordinarios de justicia[48], cuestión que dentro de nuestro sistema supone un gran problema si observamos la alta carga de trabajo que hoy afrontan nuestros tribunales de justicia. Esta situación ha generado desincentivos para la interposición de la acción, cuestión que a su vez genera un impacto en la protección efectiva y eficaz de los derechos de los titulares de datos.

Afín a esta idea es Paloma Herrera, quien sostiene que "en aquellos casos donde no se han respetado los derechos de acceso, rectificación, cancelación y oposición, y ante la

[46] El art. 16 nos menciona dos causales para dar paso a esta acción: (i) que el responsable del registro o banco de datos no se pronuncie respecto de la solicitud del requirente o titular de datos dentro de dos días hábiles o (ii) que exista una denegación por parte del responsable del banco de datos por causa distinta a la seguridad de la Nación o el interés nacional (denegación injustificada).
[47] NOGUEIRA, H. Op. Cit. p. 465.
[48] El art. 16 de la Ley N°19.628 radica la competencia en el juez de letras en lo civil del domicilio del responsable que se encuentre de turno según las reglas correspondientes, siempre y cuando se alegue amparo de los derechos contenidos en el art. 15 del mismo cuerpo. Por su parte, se faculta a la Corte Suprema para conocer de esta acción solo en el caso de que la causal invocada, para la denegación de los derechos, sea la seguridad de la Nación o el interés nacional.

carencia de una autoridad de control en Chile, ha sido difícil exigir el cumplimiento de la normativa contenida en la LPVP [Ley N°19.628]. Además, al ser el *habeas data* un procedimiento totalmente judicializado, al momento de analizar el costo-beneficio las personas deciden no perseverar y prefieren recurrir de protección en aquellos casos de trasgresión grave a sus derechos, colapsando aún más el sistema judicial chileno"[49-50]. Por otra parte, se ha señalado que "el procedimiento específicamente creado para las controversias que se susciten sobre los supuestos planteados por esta ley ha resultado prácticamente inutilizado ante las tentaciones del recurso de protección"[51].

Esto nos lleva a concluir que nuestra ley contempla si bien contempla un mecanismo de protección de datos personales dicho procedimiento no ha logrado garantizar una protección real y efectiva de los derechos de los titulares de datos, quienes se han visto en la necesidad de usar otras alternativas jurídicas para satisfacer sus pretensiones. Esta cuestión nos invita a reflexionar en torno a la necesidad de implantar, dentro de nuestro sistema, un nuevo procedimiento de protección de datos personales que sea llevado a cabo ante un órgano especializado y no frente a los tribunales ordinarios, los cuales se han visto incapacitados de llevar a cabo una labor efectiva en el conocimiento del recurso de Hábeas data. Un procedimiento especial de protección que sea de conocimiento de una autoridad de control, como la Agencia de Protección de Datos Personales, permitirá que nuestro país cuente con un sistema fuerte de protección de datos personales acercándonos al nivel internacional exigido, permitiendo que nuestro país se establezca en el marco internacional como un país seguro frente a la captación y tratamiento de datos.

II.2.2.- Recurso de Protección

Como se señaló con anterioridad, la falta de aplicación del recurso de Hábeas Data ha devenido en que se recurra, con mayor frecuencia, al uso del recurso de protección en la salvaguarda de los derechos de los titulares de datos. Lo anterior es debido a que el recurso

[49] HERRERA, P. El derecho a la vida privada y las redes sociales en Chile. *Revista Chilena de Derecho y Tecnología,* Vol. 5, N°1, 2016, pp. 87-112. p. 102.

[50] Cuestión curiosa en torno a este tema es que en Europa la expresión *habeas data* se encuentra referida a un proceso que contiene una etapa administrativa y otra judicial, mientras que en nuestro país la expresión solo dice referencia con la acción judicial contenida en el artículo 16 de la Ley N°19.628. Podemos observar, por tanto, una diferente concepción del *habeas data,* una como proceso y otra netamente como una acción frente a acciones ilegales o arbitrarias que afecten los derechos de los titulares de datos. En: HERRERA, P. Ídem, nota al pie N°31. p. 102.

[51] ROSTIÓN, I. Sobre la Ley de Protección de la Vida Privada: La importancia de una "fuente legal" y su aplicación en las personas jurídicas. *Revista Ius et Praxis,* Año 21, N°2, 2015, pp.499-520. pp. 500-501.

de protección, dentro de nuestro ordenamiento jurídico, goza de una expedita y eficaz tramitación ante las Cortes de Apelaciones, cuestión que no es observable respecto del recurso de Hábeas Data que consagra nuestra ley especial.

Es importante señalar, en primer lugar, que la protección de datos personales a nivel constitucional tiene su origen "en la jurisprudencia del Tribunal Constitucional Federal Alemán, a propósito de dos casos relativos al censo. El tribunal estimó que la protección de la dignidad de la persona humana y el libre desarrollo de la personalidad garantizaban un derecho individual a no ser instrumentalizado en su información personal para la elaboración de estadísticas oficiales"[52]. Estos fallos del Tribunal Constitucional Federal Alemán tendrán por efecto que, con posterioridad, se consagró en Europa el derecho a la protección de datos personales como un pilar del tratado que estableció una Constitución para Europa en su artículo 8, el cual dispone que las personas tienen derecho a la protección de los datos de carácter personal que le conciernan, así como también el derecho a que estos sean tratados de forma leal, para fines concretos y con base en el consentimiento de la persona afectada.

Por otra parte, en el ámbito latinoamericano, podemos destacar que diversos Estados tomaron la postura de consagrar en sus Cartas Fundamentales el derecho a la protección de los datos personales, por ejemplo, países como Argentina (artículo 43), Bolivia (artículo 130), Colombia (artículo 15), México (artículo 16, inciso segundo), Brasil (artículo 71) y Paraguay (artículo 135)[53].

Respecto de la situación particular de nuestro país se debe señalar que, hasta antes de la reforma constitucional del año 2018[54], nuestra Constitución Política de la República no contenía una mención expresa en torno a la consagración de derechos sobre datos personales. El artículo 19 N°4 de la Carta Fundamental solo hacía referencia a los derechos de protección a la vida privada y la honra de las personas y su familia. Esto implicaba que la protección de datos personales se argumentara como una derivación de aquellos derechos fundamentales contenidos en el numeral cuarto.

Con la reforma del año 2018, antes mencionada, se consagró en nuestra Constitución, como derecho fundamental, el respeto sobre los datos personales de las personas. Esta

[52] CONSEJO PARA LA TRANSPARENCIA. Experiencia comparada sobre la consagración constitucional del derecho de acceso a la información y la protección de datos personales. Cuaderno de trabajo N°18, Dirección de Estudios, 2020. p. 26.
[53] CONSEJO PARA LA TRANSPARENCIA. Idem. p. 26.
[54] Ley N°21.096 del Ministerio Secretaría general de la Presidencia que Consagra el Derecho a Protección de los Datos Personales.

consagración constitucional permitió cuadrar nuestro ordenamiento jurídico respecto no sólo de nuestra región, sino que también respecto de otros continentes. Así, desde "un punto de vista sustancial, la reforma constitucional impone diversos mandatos a diversos poderes que conforman el Estado y a los particulares, por aplicación del principio de eficacia horizontal de los derechos fundamentales. El primero de estos mandatos tiene como destinatario al legislador, quien deberá establecer la «forma» y las «condiciones» que regularán el «tratamiento» y la «protección» de datos personales.

El segundo mandato tiene como destinatario al Poder Judicial y a los órganos de la Administración del Estado que ejercen algún tipo de jurisdicción, ya sea judicial o administrativa, quienes en el ejercicio de sus funciones deberán considerar el nuevo derecho constitucional a la autodeterminación informativa y dar amparo efectivo a la protección de datos personales en cada caso que se les presente"[55].

Se ha señalado que "la decisión de reconocer explícitamente el derecho a la autodeterminación informativa en el art. 19 No. 4 de la Constitución tenía entre otros objetivos el de asegurar su tutela a través de la acción o recurso de protección, establecido en el art. 20 de la Constitución. En efecto, tanto diputados como senadores estimaban que el recurso de protección sería un medio expedito, rápido y eficaz en la protección del nuevo derecho. Esta necesidad no se encontraba argumentada o respalda especialmente, pero puede deberse a la insatisfacción relativa a un habeas data como acción legal jurisdiccional, que exige el patrocinio de abogado y se tramita ante los tribunales ordinarios. Tal como en su momento lo evaluó la Cámara de Diputados, el procedimiento actual de habeas data establecido en la Ley No. 19.628 no es eficaz para proteger los derechos de las personas, ya que "el titular de los datos tiene derecho a recurrir al juez de letras en lo civil del domicilio del responsable", lo que "implica un costo para el afectado y un tiempo de tramitación considerable que no se ajusta a las exigencias de los actuales sistemas de información"[56].

Esta consagración del derecho de protección de datos personales con rango constitucional permite a los titulares de datos optar por una vía más rápida en la protección de sus derechos, no siendo contraria a la acción que se consagra el art. 16 de la Ley N°19.628. Esta idea de compatibilidad de las acciones ya había sido reconocida por nuestra Corte Suprema aun antes de la constitucionalización del derecho en cuestión, señalando dicho

[55] ÁLVAREZ, D. La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa, Op. Cit. pp.3-4.
[56] CONTRERAS, P. El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la constitución chilena. Op. Cit. pp. 112-113

tribunal que “la existencia de un procedimiento especial contemplado en la Ley N°19.628 no obsta al ejercicio de la acción de protección, porque ésta puede ejercerse sin perjuicio de otros derechos”[57].

Lamentablemente, la compatibilidad de las acciones fue generando un efecto no pensado en los orígenes de la Ley N°19.628, toda vez que el recurso de protección ganó terreno en desmedro de la acción especial contenida en dicha norma.

Ahora bien, el uso del recurso de protección no ha estado ajeno a cuestionamientos por parte de la doctrina nacional, la cual ha sostenido que la falta de jurisprudencia relevante en la materia ha devenido en el uso del recurso de protección con resultados poco inciertos y estandarizados. Cuestión que implica resultados negativos, toda vez que no otorga un adecuado nivel de protección de los derechos de las personas[58].

Alineado con las críticas al uso del recurso de protección como mecanismo de protección de datos personales el profesor Magliona sostuvo que “no era partidario que la protección de datos personales esté amparada por la acción cautelar de derechos que establece el artículo 20” y recalcó que era conveniente tener una institucionalidad administrativa especializada para conocer la acción de Hábeas Data. Por otra parte, la consejera del Consejo para la Transparencia, Gloria de la Fuente, advirtió que el recurso de protección, si bien puede ser interpuesto sin necesidad de contar con patrocinio de un abogado, para alegar la causa sí se requiere de representación por parte de un abogado y la decisión del recurso no permite generar resolución de problemas con alcance general, como sí se puede lograr a través de las potestades de una autoridad de protección de datos personales”[59].

A raíz de lo expuesto es posible sentenciar que “ En Chile, la apuesta ha sido tener acciones judiciales sumarias que permitan obtener la defensa de los derechos de las personas ante Tribunales de Justicia. Sin embargo, como lo muestra la práctica de la aplicación de la Ley Nº19.628, los Tribunales ordinarios no presentan el mejor ambiente para la atención y solución de problemas de esta clase, más aún cuando su estructura y funcionamiento no está adecuado a ello. Con suerte, se ha podido obtener una aplicación indirecta de esta Ley mediante la interposición de acciones de protección constitucional relacionando la Ley

[57] Corte Suprema, Rol N°11256-2011, de 27 de Enero de 2012, c.6°.
[58] En dicho sentido se manifiesta, por ejemplo, Daniel Valenzuela.
[59] CONTRERAS P. Op. Cit. p.113

Nº19.628 con la garantía constitucional contemplada en el artículo 19 Nº4 de nuestra Constitución Política de la República"[60].

A pesar de las críticas enunciadas con anterioridad, la consagración del derecho a la protección de datos personales en un numeral específico del artículo 19 de nuestra Constitución, es señal inequívoca de la intención del legislador de no abandonar el mecanismo de protección que se venía privilegiando en la práctica. Es posible desprender de esta actitud del legislador la voluntad de reforzar (ante la falta de una entidad especializada que conozca de procedimientos especiales) el recurso de protección como la vía idónea para salvaguardar los intereses de los titulares de datos dentro de nuestro sistema.

II.3.- FALTA DE AUTORIDAD

El punto más relevante, en cuanto a las críticas que se puede realizar a nuestra ley especial sobre datos personales y en cuanto al objeto de este trabajo, es la falta de consagración de una autoridad o entidad pública autónoma y especializada, con facultades fiscalizadoras y sancionadoras, encargada de conocer los conflictos originados por el tratamiento de datos personales dentro de nuestro ordenamiento jurídico. Nuestra "Ley de Datos Personales no contempló la creación de un organismo público encargado de velar por el cumplimiento de sus disposiciones. Se limitó a establecer determinados principios en cuanto al tratamiento de datos personales por parte de organismos públicos y privados, y entregó a la justicia ordinaria el conocimiento de los conflictos que se suscitaran"[61]. Producto de esto, "al no generarse un órgano de supervisión y control encargado de velar por el cumplimiento de la ley, el sistema de protección estructurado es muy débil"[62].

Así, desde el momento en que la ley N°19.628 entró en vigor, uno de los consensos que existió, en materia de protección de datos, es que Chile requiere de una autoridad de control (preferentemente autónoma y especializada) que se haga cargo de promover, educar e informar a los ciudadanos sobre su derecho a la vida privada y a la protección de sus datos personales, fiscalizar el cumplimiento de la ley y sancionar las infracciones, entre otras funciones[63]. En el mismo sentido, Francisco Cumplido, al analizar un anteproyecto de ley sobre

[60] ONG DERECHOS DIGITALES. Minuta de discusión: Proyecto de ley que introduce modificaciones a la Ley N°19.628, sobre protección de la vida privada y protección de datos de carácter personal (Boletín N°8143-03). p. 5.
[61] MATUS, J. Op. Cit. p. 201.
[62] NOGUEIRA, H. Op. Cit. p.465.
[63] ÁLVAREZ, D. Op. Cit. p.56.

protección de datos personales elaborado por el Ministerio de Justicia en el período 1990-1994, categóricamente sostuvo que "llegamos a la conclusión de que, para que pudiera ser efectiva y real la protección de los datos personales, era indispensable establecer un servicio del Estado que contribuyera a la protección de esos datos personales"[64].

Lo anterior no solo se ha puesto de relieve desde el mundo jurídico, sino que también desde agrupaciones sociales que pretenden hacer frente a los problemas suscitados en torno a la protección de datos personales. Así, "Desde la sociedad civil, el grupo Res Pública, en su documento «95 propuestas para un Chile mejor» recoge también esta preocupación, proponiendo una serie de modificaciones a la legislación nacional sobre protección de datos personales, entre las cuales mencionan expresamente la «creación de una agencia autónoma e independiente que fiscalice, promueva y garantice la aplicación de la ley en lo que se refiera a datos personales. Bajo su supervisión estarían los organismos privados y públicos que manejen bases de datos con información personal, y mantendría un registro de las bases existentes con la identificación de sus responsables"[65].

"Como se puede apreciar, constituye hoy una opinión generalizada y mayoritaria, la necesidad de contar con una autoridad de control en materia de protección de datos personales en Chile. El disenso se produce al momento de determinar qué órgano debiera ejercer dicha función"[66].

En torno a este último punto se puede señalar que, lamentablemente, prácticamente en su totalidad los proyectos modificatorios de la actual Ley no han contemplado la creación de un organismo autónomo y especializado, sino que han optado por otorgar facultades fiscalizadoras y sancionatorias a otros órganos públicos ya existentes en nuestro ordenamiento jurídico. Un primer ejemplo de esto viene dado por el proyecto modificatorio contenido en el Boletín N°6120-07[67], presentado en el primer gobierno de la presidenta Michelle Bachelet, el cual, en lo que a este ensayo respecta, no contemplaba la creación de un organismo autónomo fiscalizador en la materia, sino que entregaba las facultades de control y fiscalización al Consejo para la Transparencia.

---

[64] CUMPLIDO, F. Análisis del anteproyecto de ley sobre protección de datos personales elaborado por el Ministerio de justicia (1990-1994). En: ÁLVAREZ, D. Idem.
[65] ÁLVAREZ, D. Acceso a la información pública y protección de datos personales: ¿puede el consejo para la transparencia ser la autoridad de control en materia de protección de datos? Op. Cit. p. 58.
[66] ÁLVAREZ, D. Idem. p. 60.
[67] Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/veto.aspx?prmID=6505&prmBOLETIN=6120-07

Un segundo ejemplo viene dado por el proyecto de ley que establecía medidas para incentivar la protección de los derechos de los consumidores contenidas en el Boletín N°12409-03[68], presentado bajo el segundo mandato del presidente Sebastián Piñera, el cual pretendía entregar al Servicio Nacional del Consumidor (en adelante "SERNAC") la competencia para conocer de los asuntos en torno a la protección de los datos personales, con especial énfasis en la regulación respecto de los privados que realizan tratamiento de datos personales.

Ambos proyectos antes señalados, si bien significaban avances importantes en la materia, fueron objeto de ciertas críticas que no permitieron llevar a cabo los planes modernizadores que contenían. Las críticas apuntaban principalmente, como se ha señalado reiteradamente, a la idea de que el órgano encargado de la fiscalización y promoción de la protección de datos personales no debía ser un ente ya vigente dentro de nuestro sistema, sino que debían recaer tales facultades en un órgano independiente con características especializadas en la materia.

II.3.1.- Actuación del Consejo para la Transparencia como autoridad de control en materia de protección de datos personales.

Ante la falta de autoridad en materia de protección de datos personales el Consejo para la Trasparencia (en adelante también "CPLT" o "el Consejo") ha asomado como el órgano predilecto en el cual radicar las facultades fiscalizadoras en la materia. Esto se ha dado, principalmente, por la labor que ha cumplido el Consejo en materia de datos personales respecto de los organismos del sector público.

Esta idea deviene del hecho de que el artículo 33 letra m) de la Ley 20.285 sobre Acceso a la Información Pública (en adelante, indistintamente «Ley de Transparencia o «Ley 20.285») estableció, dentro de las competencias del Consejo para la Transparencia, la obligación de velar por la aplicación y el cumplimiento de la Ley 19.628 respecto de la gestión de los órganos de la Administración del Estado.

En favor de la idea de establecer al Consejo como el organismo garante de la protección de datos personales en nuestro sistema se han señalado una serie de puntos

[68] Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12940&prmBoletin=12409-03

relevantes. En primer lugar, se ha sostenido que esto implicaría menor gasto público y una menor burocracia toda vez que concentrar la protección de datos en el CPLT permitirá absorber la demanda que supone la protección de datos, especialmente para resolver solicitudes y reclamaciones, investigar y determinar las infracciones, prestar asesoría técnica, difundir y capacitar, supervigilar los modelos de prevención, entre múltiples funciones. Por otra parte, esto nos permitiría aprovechar las economías de escala y la eficiencia de concentrar las competencias de transparencia y protección de datos, aprovechando a su vez la capacidad instalada de una institución con 10 años de rodaje y el conocimiento sobre la protección de datos personales respecto de los órganos públicos[69].

En segundo lugar, se ha señalado que el hecho de que el Consejo asuma la tarea de protección de datos personales no afectaría sus funciones respecto al acceso a la información pública, debido principalmente a que la entrada de casos por esta materia no representaría cifras abrumadoras que no implicarían un aumento en la carga de trabajo que dañe la labor de la institución[70]. En tercer lugar, atribuir las competencias para la protección de datos personales a una nueva Agencia, distinta del CPLT, afectaría directamente la Transparencia en nuestro país, pues se entorpecería el derecho al acceso de la información pública, dilatando resoluciones, judicializando el derecho y dañando la seguridad jurídica. Una sola institución a cargo de la materia incrementa los niveles de certeza jurídica en los criterios para garantizar de manera armónica la Protección de Datos Personales y la Transparencia, no poniendo en riesgo el correcto desarrollo de ambas materias debido a interpretaciones disímiles o contradictorias[71].

En la misma línea se sostiene que concentrar las competencias en un órgano elimina la conflictividad entre agencias y los riesgos de contradicción entre distintas instituciones, mejorando la eficiencia. Además del hecho de que “la experiencia internacional muestra una

---

[69] CONSEJO PARA LA TRANSPARENCIA. Fundamentos para definir al Consejo para la Transparencia como la autoridad de control en materia de protección de datos personales, 2019, p. 1. [En Línea]: https://www.consejotransparencia.cl/wp-content/uploads/estudios/2020/01/Fundamentos-para-definir-al-Consejo-como-la-autoridad-PDP.pdf [Consulta: 27 Octubre 2021].

[70] “Si consideramos una proyección comparativa de la tasas de casos en PDP per cápita que tramitan las principales agencias de Protección de Datos Personales en el mundo (con décadas de desarrollo, pedagogía y concientización), llegamos a un promedio internacional de 11.7 casos cada 100 mil habitantes.
Por su parte, en Chile, el año 2018 el CPLT, en acceso a la información, tramitó 36 casos cada 100 mil habitantes. El CPLT ha venido sostenidamente abordando un aumento importante de casos en Derecho de Acceso a la Información, si en el año 2009 se recibieron 629 casos, en el 2013, a cinco años de su entrada en funcionamiento, ingresaron 2.320 casos. En el año 2018 se recepcionaron 6.679 casos, lo que representó un aumento de un 45% respecto al 2017 y para el 2019 se proyecta que se superarán los 8.000 casos. Este permanente y significativo incremento de la demanda, lejos de mermar su rendimiento, ha fortalecido su capacidad de resolución y su jurisprudencia”. En: Fundamentos para definir al Consejo para la Transparencia como la autoridad de control en materia de protección de datos personales, *Op. Cit.* p. 3.

[71] Ídem. p. 3.

tendencia clara: autoridades en diversos países comparten las competencias vinculadas al derecho de acceso a la información y la protección de datos personales. Una revisión del derecho comparado permite observar que, aquellos países con una regulación más avanzada en materia de protección de datos personales han optado por diseñar institucionalidades que comparten ambas competencias. Tanto en Europa como en América Latina, se ha optado por la creación de autoridades con competencia común en ambos derechos, a efectos de poder compatibilizarlos de manera adecuada"[72].

Así, los argumentos a favor expresados pueden resumirse en la idea de que el CPLT es considerada como una autoridad que puede hacerse cargo de la fiscalización, promoción y sanción de las cuestiones suscitadas en torno a la protección de datos personales con menor gasto público[73], mayor eficiencia y eficacia, y remarcando la idea de independencia y autonomía de la autoridad de control.

Ahora bien, la idea de establecer al Consejo como la autoridad en materia de protección de datos personales también ha sido objeto de críticas que permiten señalar que optar por dicha solución no es el camino idóneo que nuestro país debiese tomar.

Se ha cuestionado la idea, en primer lugar, en base a la incompatibilidad de áreas de resguardo que se radicarían en el CPLT, cuestionándose el hecho de establecer en un solo órgano el acceso trasparente a la información y la protección de datos. "Una perspectiva —la de la Ley 20.285— apunta al objetivo de accesar actos administrativos, contratos administrativos, documentos y resoluciones, para generar transparencia y publicidad ante el requerimiento de cualquier ciudadano y sin expresión de causa o motivo; la otra —la de la Ley 19.628— busca acceso para asegurar el control, la autodeterminación y la reserva de los datos o antecedentes nominativos de una persona determinada, legitimada activamente por estar en juego sus propios antecedentes personales, que le pertenecen y que lo identifican actualmente o lo hacen identificable a futuro"[74].

Pareciera ser que "la relación entre la protección de datos personales o el habeas data y el derecho de acceso a la información de la gestión del Estado no son, de modo alguno, «las

---

[72] Ídem. p. 7.

[73] Se ha señalado que la creación de una nueva autoridad que se encargue de la protección de datos generaría un costo fiscal de $1.428 millones anuales en régimen. En cambio, ampliar las atribuciones del CPLT, implicaría un gasto fiscal total en régimen de 874 millones anuales, es decir, implicaría un ahorro fiscal anual de casi $600 millones.
En; El debate sobre datos personales vuelve cardado de dudas sobre su financiamiento. En Pauta en internet. 30 de Junio, 2021. https://www.pauta.cl/economia/proyecto-datos-personales-costos-fiscales-consejo-para-transparencia [Consulta: 23 Octubre 2021].

[74] JIJENA, R. Op. Cit. p. 63.

dos caras de la misma moneda». De hecho, la cara del habeas data de la Ley 19.628 es esencial en un mundo no relacionado con la gestión de los servicios públicos, es decir, en el sector privado y para que las personas controlen sólo el uso de sus datos personales. Y a propósito de la gestión de los órganos del Estado, con el norte de transparentarla para evitar faltas a la probidad y corrupción que es la razón de ser de la Ley 20.285, tanto el artículo 8 de la Constitución de 1980 como los artículos 7 y 21 de la ley de acceso son claros en el sentido de la necesidad de restringir y resguardar la reserva y confidencialidad de los datos personales. Lo que en verdad ocurre que son monedas o billetes de diverso cuño y de distinto valor que sirven para pagar conflictos jurídicos diversos. Además, es posible de sostener que lo establecido en el artículo 33 letra m) es una competencia limitada. Esta facultad no se puede extender al punto de considerar que estamos frente a la nueva Autoridad o Agencia de Protección de Datos chilena, y de creer que el Consejo posee competencia procesal y administrativa para conocer de reclamos en que se invoque la no aplicación o respeto de la Ley 19.628 por los servicios públicos"[75].

Por su parte, Daniel Álvarez sostiene que, respecto de entregar las facultades al CPLT, un informe del Centro de Sistemas Públicos de la universidad de Chile, encargado por el propio CPLT, realizó una crítica en base a 4 puntos fundamentales. En primer lugar, se señaló que la experiencia internacional nos permite establecer la prevalencia de entidades autónomas o agencias exclusivas en materia de protección de datos (tomando como ejemplo paradigmático la Agencia Española de Protección de Datos Personales). En segundo lugar, se señaló que existiría una diferencia de "negocios", es decir, hay una contraposición entre los principios que inspiran la transparencia y el acceso a la información pública que serían contradictorios con la idea de privacidad o autodeterminación informativa que está detrás de los regímenes de protección de datos personales. En tercer lugar, se cuestiona la capacidad del CPLT se fallar contra sí mismo (argumento más cuestionable). Finalmente, en cuarto lugar, se cuestiona que el establecimiento de una agencia multisectorial genera problemas en torno al gran poder que tendría, lo que la hace susceptible a mayores focos de captura por parte de los particulares y del poder político[76].

De lo antes expuesto es claro observar que "sigue pendiente y suena fuerte el afán del Consejo para la Transparencia por desnaturalizarse, y transformarse en la nueva autoridad chilena de protección de datos personales. Es decir, dejar de transparentar documentos del

[75] JIJENA, R. Idem. p. 89.
[76] ÁLVAREZ, D. Op. Cit. pp. 73-76.

Estado para velar por la privacidad y confidencialidad de los datos personales de los chilenos —ya no tan sólo en el contexto de la gestión de los servicios públicos—, sin tener la idoneidad ni la preparación necesaria"[77].

Todo esto aun cuando, "lamentablemente, siguen sin hacerse cargo de los argumentos en contrario de un informe neutral de una Escuela de Ingeniería que ellos mismos encargaron. En las páginas 110 y 111 del estudio, de forma clara y directa, se consigna que no es idóneo tener en una misma institución las funciones de protección de datos y de acceso a la información; que la experiencia internacional recogida demuestra que en su gran mayoría los temas los abordan agencias diversas; que es crítico el desconocer que se trata de «negocios» muy distintos, considerando los principios involucrados, las funciones que deben desarrollarse (transparentar una y resguardar la confidencialidad y privacidad de los datos personales), los sectores donde operan (no hay acceso en el sector privado) y que los conflictos de intereses se presentan también en ámbitos muy diversos"[78].

II.2.3.- SERNAC como autoridad en materia de protección de datos personales.

Otro organismo que se ha pretendido establecer como la autoridad encargada de la protección de los datos personales es el Servicio Nacional del Consumidor (en adelante también "SERNAC"). Esto se explica, en gran medida, debido a la labor de protección que realiza la entidad respecto de las diversas problemáticas que surgen en la relación de los consumidores con las empresas; en dicha relación se pueden evidenciar problemas en torno a los datos personales, por ejemplo, debido a la captación de datos que hace el *retail* al momento de la venta de productos o servicios a los consumidores.

Si bien se ha señalado, hasta hace poco tiempo, que la protección de datos personales y el derecho del consumidor constituían compartimentos separados, cada uno con su propio estatuto legal[79], el desarrollo de la economía en línea ha alterado profundamente esta relación. Los términos y condiciones con que los proveedores pretenden regir la contratación de bienes

[77] JIJENA, R. Idem. p. 93.
[78] JIJNEA, R. Idem. p. 93-94.
[79] El primero relacionado con el resguardo de derechos fundamentales como la honra y la vida privada. El segundo, relacionado con el derecho de los consumidores frente a los abusos de los proveedores en una economía de mercado.

y servicios que ofrecen en línea incluyen sin falta cláusulas sobre uso y tratamiento de datos personales[80].

El último gran esfuerzo tendiente a unir el mundo de la protección de los derechos de los consumidores y las materias relacionas con datos personales viene dado por el proyecto de ley modificatorio de la Ley N°19.496 (que establece las normas sobre protección de los derechos de los consumidores)[81], en el cual se pretende otorgar facultades de protección de datos personales al SERNAC a través de la introducción de un nuevo artículo 15 bis dentro del cuerpo normativo antes mencionado. Dicho artículo señala, en su inciso primero, que "las normas relativas al tratamiento de cualquier tipo de datos personales de los consumidores, incluyendo especialmente los de carácter comercial, contenidas en la ley N° 19.628, sobre protección de la vida privada, en especial en el Título III "De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial", y demás normas legales relacionadas, se considerarán normas especiales de protección de los derechos del consumidor, especialmente para los efectos de lo dispuesto en los artículos 2° bis, 58 y 58 bis de la presente ley"[82].

Según consta en informe de la comisión de economía, fomento, micro, pequeña y mediana empresa, protección de los consumidores y turismo, "la introducción de un nuevo articulado en dichos términos ratifica la competencia del SERNAC para monitorear y supervisar en el cumplimiento de sus competencias (art. 58 y art. 58 bis) y ejercer acciones colectivas (art. 2 bis) en casos de daño a los consumidores por infracción a la ley N° 19.628.

---

[80] MOMBERG, R. y MORALES, M. Las cláusulas relativas al uso y tratamiento de datos personales y el artículo 16 letra g) de la Ley 19.496 sobre Protección de los Derechos de los Consumidores. *Revista Chilena de Derecho y Tecnología,* Vol. 8 N°2, 2019, pp. 157-180. p. 158.

[81] Proyecto contenido en el Boletín N°12409-03. Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12940&prmBoletin=12409-03

[82] El artículo continua señalando que " Los proveedores que realicen el tratamiento de cualquiera de los datos mencionados en el inciso anterior deberán dar estricto cumplimiento a las normativas que allí se señalan. Para estos efectos, deberán implementar las medidas necesarias para garantizar la seguridad y la reserva en el tratamiento de datos, con especial resguardo respecto de los fines para los cuales fueron autorizados por su titular.
En el supuesto de que los proveedores reporten una violación de seguridad de sus bases de datos o de aquellas de las que se sirvan y que contengan información de sus clientes o usuarios, será mandatoria la entrega de información a los consumidores de lo ocurrido, dentro de 24 horas contadas desde el referido reporte.
Esta comunicación se deberá efectuar de forma digital e incluirá las medidas de seguridad adoptadas en momentos previos y posteriores a la ocurrencia del hecho. En caso de no prosperar esta vía de contacto, esta misma información se pondrá en conocimiento del consumidor a través de medios físicos, telefónicos u otros idóneos que garanticen celeridad, dentro de un plazo de 72 horas contado desde el reporte señalado en el inciso anterior.
Las consultas y reclamos suscitadas con ocasión de este tipo de incidentes se canalizarán a través del servicio de atención a los clientes que disponga cada proveedor.
Sin perjuicio de lo consagrado en los incisos anteriores, el responsable tendrá la obligación de informar, a petición del consumidor, la fuente de legitimidad del tratamiento de sus datos y de respetar, en todo caso, la finalidad para la cual fueron recolectados o almacenados.".

Este principio venía siendo uniformemente reconocido por las cortes en las acciones colectivas de SERNAC en la materia (ej. Corte Suprema Rol 4903-2015 y Rol 1533-2015)"[83].

A favor de la idea de establecer al SERNAC como autoridad de control se ha señalado que "la experiencia comparada como la europea, reconoce un rol relevante a los órganos de consumo en la protección de los intereses colectivos y difusos de los consumidores en materia de datos personales. El Parlamento Europeo promulgó una Directiva reciente que exige a sus países miembros disponer de acciones colectivas, similares a las del SERNAC, como mecanismo efectivo de tutela judicial en materia de "protección de datos", "regulación de la sociedad de la información", "comunicaciones electrónicas" y "condiciones generales de la contratación"[84]. Sosteniéndose además que el SERNAC cuenta con las competencias, experiencia e interés de la ciudadanía para ejercer las facultades necesarias en la materia, lo cual ya se ha evidenciado, según su director don Lucas Del Villar, en el ejercicio de acciones en defensa de los datos personales de los consumidores en el caso "cartolazo" del Banco de Chile; la filtración de datos de clientes en la empresa Claro; la demanda colectiva contra Correos de Chile por filtrar datos de tarjetas de créditos de clientes por su operador en Miami, entre otros[85].

Ahora bien, al igual que lo acontecido con el CPLT la idea de establecer la Sernac como la autoridad de protección de datos personales ha recibido críticas por parte de quienes consideran que esta entidad no es la adecuada para realizar dicha labor, ya sea porque se considera que el CPLT es quien debe llevar a cabo dicha tarea, o bien, porque se considera que se debe optar por la creación de una entidad especializada.

Así, en torno al proyecto modificatorio antes señalado, la Asociación Chilena de Empresas de Tecnologías de Información A.G (ACTI A. G) señaló que "El Sernac no es el organismo más idóneo para conocer de materias de datos personales (…) está en contra de la normativa internacional, considerando que para que la normativa de datos personales de Chile sea considerada de adecuado estándar, se requiere que el organismo que vela por los datos personales sea autónomo e independiente, situación en la que no se encuentra el

[83] INFORME DE LA COMISIÓN DE ECONOMÍA, FOMENTO, MICRO, PEQUEÑA Y MEDIANA EMPRESA, PROTECCIÓN DE LOS CONSUMIDORES Y TURISMO RECAÍDO EN EL PROYECTO DE LEY QUE ESTABLECE MEDIDAS PARA INCENTIVAR LA PROTECCIÓN DE LOS DERECHOS DE LOS CONSUMIDORES. p. 6. [En Línea]: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12940&prmBoletin=12409-03 [Consulta: 28 Octubre 2021].
[84] DEL VILLAR, L. El SERNAC y protección de datos, 2021. [En Línea]: https://www.sernac.cl/portal/604/w3-article-62885.html [Consulta: 28 Octubre 2021].
[85] DEL VILLAR, L. Idem.

Sernac"[86]. Por su parte, el profesor y abogado Renato Jijena sostuvo que permitir al Sernac que, sin expertice, pondere una brecha de seguridad, o que determine cuando cualquier tratamiento de datos vulnera -o no- la confidencialidad o secreto, la finalidad o la falta de diligencia que exigen el derecho hoy vigente, so pretexto de la conveniencia de interponerse acciones colectivas, es errado. Señalando además que convertir al SERNAC en una mini autoridad de protección de datos no es lo adecuado ya que esto no se condice con las exigencias que la OCDE plantea en la materia[87].

Finalmente, la Cámara Chileno Norteamericana de Comercio (Amcham Chile) realizó comentarios al artículo 15 bis, que pretendía introducir el proyecto modificatorio de la ley N°19.496, en el sentido de que esta norma no permitiría que Chile opte a ser calificado como legislación adecuada por la Unión Europea y tener una legislación de privacidad suficiente para estándares OCDE. Esto debido a que "uno de los requisitos esenciales bajo el Reglamento General de Protección de Datos de Europa (artículo 45.2.b) para evaluar la adecuación del nivel de protección de una jurisdicción que permita el libre flujo de datos personales – en este caso, entre Chile y Europa – es "la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país". La conformación administrativa de Sernac, cuyo director es nombrado por el Presidente de la República y siendo de su exclusiva confianza, determinan que Sernac no cumpla con el requisito administrativo de independencia, esencial para lograr la ansiada declaración de adecuación (de la que hoy goza, por ejemplo, Argentina y Uruguay)"[88].

Con lo expuesto podemos señalar que en nuestro ordenamiento no se ha podido llegar al consenso necesario en torno a establecer al SERNAC como la entidad encargada de velar por la protección de los datos personales, siendo posible establecer la misma aseveración respecto del CPLT, es decir, que el mecanismo idóneo para la debida protección de los datos personales, que adecue las necesidades expuestas por los especialistas, es la adopción de una entidad independiente y especializada en nuestro sistema. La adopción de una autoridad de control autónoma nos permitirá alinearnos con los modelos de países más desarrollados en materia de protección de datos y permitirá que no se radiquen las competencias de conocimiento de estos temas en autoridades que desempeñan otro tipo de funciones dentro

[86] [En Línea]: https://acti.cl/wp-content/uploads/2021/04/Declaracion-ACTI-SERNAC_firmada.pdf [Consulta: 26 Octubre de 2021].
[87] JIJENA, R. Datos personales y consumidores; ojo al cuidador. Diario Financiero en internet, 2021. [En Línea]: https://www.df.cl/noticias/opinion/columnistas/datos-personales-y-consumidores-ojo-al-cuidador/2021-05-05/193731.html [Consulta: 28 Octubre de 2021].
[88] AMCHAM CHILE. Comentarios de AmCham Chile a artículo 15 bis del Boletín 12.409-03. p. 1-2.

de nuestro sistema; involucrar a autoridades que desempeñan otro tipo de funciones (aunque puedan resultar similares) puede implicar, por una parte, un problema de falta de protección eficaz por no contar con el conocimiento especializado o, por otra parte, un problema de falta de protección a raíz de la demora en el conocimiento de las causas que se presenten, cuestión que se relaciona de forma directa con el exceso de carga de trabajo que puede implicar el conocimiento de una diversidad de materias.

CAPÍTULO III: AGENCIA DE PROTECCIÓN DE DATOS PERSONALES[89]

Es claro que de lo expuesto en los anteriores capítulos que las falencias de nuestra legislación se deben, en gran parte, a la falta de un órgano o autoridad especializada. Esto es grave si consideramos que "es fundamental que los Estados cuenten con organismos garantes de acceso a la información pública y la protección de datos personales, dotados de independencia y recursos, que sean promotores de estos derechos y que faciliten la apertura de la función pública a fin de reforzar la confianza ciudadana en las instituciones. Los órganos garantes son instituciones especializadas e imparciales que garantizan el ejercicio de un derecho o la protección de éstos"[90]. En especial cuando de acuerdo con "los estándares internacionales, tanto el acceso a la información como la protección de datos personales exige una institucionalidad independiente y autónoma del Poder Ejecutivo para poder resolver y sancionar los incumplimientos a la ley, tanto respecto de privados como de organismos públicos"[91].

Es fácil observar en nuestro país que "desde antes de la entrada en vigencia de la Ley Nº19.628 sobre Protección de la Vida Privada, se discute acerca de la necesidad de establecer una autoridad pública que se encargue de fiscalizar el cumplimiento efectivo de sus disposiciones"[92]. Esta situación (la falta un ente protector y fiscalizador) ha generado la casi completa ausencia de mecanismos de *enforcement* (observancia forzada) de los derechos consagrados en la Ley N°19.628. La ausencia de una autoridad de control o un órgano especializado (como se exige en el sistema europeo) con capacidad para fiscalizar ha creado

[89] Análisis realizado en base al estado de tramitación a fecha 24 de Junio de 2021 del Boletín N°11.144-07.
[90] CONSEJO PARA LA TRANSPARENCIA. Experiencia comparada sobre la consagración constitucional del derecho de acceso a la información y la protección de datos personales. Op. Cit. p. 29.
[91] CONSEJO PARA LA TRANSPARENCIA. Idem. p. 29.
[92].ÁLVAREZ, D. Acceso a la información pública y protección de datos personales: ¿puede el consejo para la transparencia ser la autoridad de control en materia de protección de datos?. Op. Cit. p. 52

en nuestro sistema serios problemas de especialización, demora en la tramitación de causas y dificultades en el acceso a la justicia para los titulares de datos que resultan afectados[93].

En tal sentido, Raúl Arrieta ha señalado con gran acierto que "el hecho de no contar con una autoridad independiente que se encuentre permanentemente velando por el cumplimiento de la ley tanto por parte de los organismos públicos como privados, que tenga la posibilidad de aplicar sanciones por el incumplimiento y que tenga un fuerte rol de promoción de la protección de datos personales, es un vacío que quizás formalmente aparece como la mayor dificultad de Chile para cumplir el estándar internacional exigido"[94].

Así, con el objeto de ajustar la realidad chilena a una tendencia internacional creciente en materia de protección de datos se ha propuesto, por gran parte de la doctrina especializada y organismos no gubernamentales con interés en la materia, la creación "de la institución de una agencia de protección de datos, esto es, una autoridad pública, autónoma e independiente, dotada de las competencias y herramientas eficaces para velar por el adecuado cumplimiento de las normas relativas al tratamiento de datos, de forma constante y activa"[95]. Todo lo anterior en atención a la resolución efectiva de las problemáticas que la nueva era digital supone en materia de datos personales.

Con esto, resulta fundamental el estudio de una nueva institucionalidad en torno a la protección de los datos personales en nuestro país, detallando su estructura y funcionamiento para entender cómo nos preparamos para afrontar el tratamiento masivo de datos al que nos vemos expuestos en una era digital como la que vivimos.

III.1.- CREACIÓN DE LA AGENCIA

Lo expuesto en el apartado anterior ha cambiado con motivo del último proyecto modificatorio de la Ley N°19.628 contenido en el Boletín N°11.144-07, denominado "Proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales". Dicho proyecto fue ingresado el 15 de Marzo de 2017 al

[93] LARA, J., VERA, F. y SOTO, B. Op. Cit. pp. 14-15.
[94] ARRIETA, R. Chile y la protección de datos personales: Compromisos internacionales. *VV.AA, Chile y la protección de datos personales: ¿están en crisis nuestros derechos fundamentales?,* Ediciones Diego Portales, 2009. p. 21. En: ÁLVAREZ, D. Acceso a la información pública y protección de datos personales. ¿puede el consejo para la transparencia ser la autoridad de control en materia de protección de datos?, Op. Cit. p. 58.
[95] LARA, J., VERA, F. y SOTO, B. Op. Cit. p. 31.

Senado, siendo posteriormente refundido con un proyecto que versaba sobre la misma materia contenido en el Boletín N°11.092-07.

La novedad de este proyecto, además de reformular en gran parte la actual ley sobre datos personales, radica en que contempla la creación de una Agencia de Protección de Datos Personales (en adelante también la "Agencia"). Tal como señala el proyecto modificatorio de la Ley N°19.628 contenido en el Boletín 11.144-07 (en adelante también el "Proyecto" o "proyecto modificatorio"), para efectos de velar por la protección de los derechos y libertades de las personas titulares de datos y por el adecuado cumplimiento de las normas relativas al tratamiento de datos, es un consenso entre la doctrina la necesidad de contar con una autoridad de control dotada de facultades para regular, supervisar, fiscalizar y, en última instancia, sancionar los incumplimientos a la normativa imperante que cometan los encargados de datos. Esta cuestión se plantea como importante teniendo en consideración que nuestra actual Ley no contempla un organismo encargado de velar por el cumplimiento de los derechos establecidos en el mismo cuerpo legal; la falta de un organismo especializado ha devenido en que la protección de los derechos sobre datos personales sea escasa y poco efectiva.

Así, es "destacable la creación de la Agencia de Protección de Datos, entidad especializada cuya instauración fue evitada en otras iniciativas, para el conocimiento de estas materias. Según se observa en el proyecto, tiene las facultades necesarias para cumplir con su función, tales como dictar instrucciones y normas generales obligatorias, fiscalizar el cumplimiento de las disposiciones de la ley, resolver reclamos de los titulares de datos en contra de los responsables de los mismos, ejercer la potestad sancionadora sobre entidades privadas, determinar infracciones de órganos públicos y requerir a la Contraloría la instrucción de los sumarios administrativos o investigaciones sumarias y, en general, acciones de cooperación y asesoría"[96].

Con la confección e instauración de una agencia, tal como se concibe en el Proyecto original modificatorio, nuestro país logrará adecuar su sistema de protección de datos personales de acuerdo con los estándares internacionales en los cuales podemos observar la existencia de organismos autónomos y especializados, con funciones similares a las que se pretenden conferir a la nueva Agencia de Protección de Datos Personales. En tal línea se

[96] VERGARA, M. Chile: comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la agencia de protección de datos personales. *Revista Chilena de Derecho y Tecnología,* VOL. 6 Núm. 2, 2017, pp.135-152. p. 150.

pronunció nuestra Corte Suprema, la cual en su informe dirigido al Senado sostuvo que el Proyecto de ley constituía un esfuerzo por aunar y concretar la necesidad de actualizar el modelo y la institucionalidad de la protección de datos personales en nuestro país, actualización que se logra a través de una modificación exhaustiva de la Ley N°19.628 que permite adecuarla a los estándares y principios vigentes en la materia, los requerimientos de la OCDE y los de la comunidad internacional[97].

III. 2.- NATURALEZA JURÍDICA DE LA AGENCIA

La Agencia de Protección de Datos Personales se consagra, en el artículo 30 del Proyecto, como un organismo público autónomo[98], de carácter técnico, descentralizado, con personalidad jurídica y patrimonio propio, encargado de velar por el cumplimiento de la normativa relativa al tratamiento de los datos personales y su protección. La Agencia estará sometida a la supervigilancia del Presidente de la República a través del Ministerio de Hacienda, además de estar afecta al Sistema de Alta Dirección Pública establecido en la Ley N° 19.882[99].

Como ya se ha señalado, esta consagración de la Agencia va en el camino correcto, toda vez que se pretende la creación de una entidad diferente y especializada, sin sucumbir a las ideas de algunos sectores de radicar esta función en la Contraloría General de la República, el SERNAC, el CPTL (como extensión de lo que ya efectúa respecto del sector público) o bien, el Servicio de Registro Civil el cual lleva actualmente el registro de banco de datos del sector público según el artículo 22 de la ley vigente[100-101].

Respecto de la necesidad de dotar de autonomía al órgano encargado de la supervigilancia de los derechos sobre datos personales se manifestó, por ejemplo, la ex Coordinadora de Mercado de Capitales y Finanzas Internacionales del Ministerio de Hacienda, quien en la discusión dentro de la Comisión de Constitución, Legislación, Justicia y

[97] CORTE SUPREMA. Informe proyecto de ley N°5-2017, 2017. p. 2.
[98] El carácter de autónomo vino dado por la modificación que realizó la Comisión de Constitución, Legislación, Justica y Reglamento en su primer informe respeto del proyecto modificatorio.
[99] El mismo artículo nos señala que el domicilio de la Agencia se radicará en la ciudad de Santiago.
[100] VERGARA, M. Op. Cit. p. 141.
[101] "El artículo 22 de la actual ley establece el deber del Servicio del Registro Civil e Identificación de llevar un registro de banco de datos de personas a cargo del organismo público, no observándose en la regulación propuesta, a primera vista, la pervivencia de este registro, a pesar de que es una norma fundamental para la transparencia e información que se consagra en el artículo 21 del proyecto". En: VERGARA, M. Op. Cit. p. 147.

Reglamento (en adelante también “la Comisión”) se desempeñó como asesora, señalando que el órgano pretendido cumple con los principios que establece el Reglamento de la Unión Europea en materia de protección de datos, uno de los cuales consiste en el hecho de que la autoridad de control sobre datos personales cuente con total independencia en el desempeño de sus funciones y en el ejercicio de los poderes, de conformidad a la ley que la crea[102].

Por su parte, el Presidente de la Comisión, Honorable Senador señor Harboe, sostuvo que, “en relación a la autonomía, ésta no es sinónimo de independencia. Relató que nuestra Carta Fundamental cuenta con órganos de carácter autónomo, que operan sobre la base del poder decisorio, que es independiente de la autoridad política. Ejemplos de ello lo constituye el Consejo de Defensa del Estado, la Fiscalía Nacional Económica. Subrayó que la clave en esta materia está dada por el hecho de que el nombramiento de su Director y las causales de remoción están establecidas por ley. Unido a lo anterior, agregó, la Agencia debe tener un grado de independencia del poder político”[103].

Sumado a lo anterior, “el asesor del Ministerio de Hacienda, señor Godoy, recordó que a esta Agencia que se le está otorgando autonomía legal, situación que se expresa en dos materias centrales, a saber:

- Es un organismo público descentralizado con personalidad jurídica y patrimonio propio;

- Está sujeto a la supervigilancia del Presidente de la República.

Recalcó que se optó porque la Agencia esté bajo la supervigilancia del Presidente de la República, a través del Ministerio de Hacienda. Ello no significa que esté bajo la tutela del Ministro respectivo. Subrayó que todas las decisiones que adopte la institución son completamente autónomas y solo están sujetas al control jurisdiccional”[104].

Aseveró que lo anterior corresponde a la misma situación jurídica que ocupa la figura de la Fiscalía Nacional Económica. Agregó que los criterios de autonomía que establece

[102] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Informe 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 Nos. 11.092-07 y 11.144 - 07, refundidos. p.425. [En Línea]: https://www.camara.cl/legislacion/ProyectosDeLey/informes.aspx?prmID=11661&prmBOLETIN=11144-07 [Consulta: 24 Septiembre 2021].
[103] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Ídem. p. 430.
[104] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Ídem. p.441.

nuestra legislación dicen relación con los sistemas de nombramiento de las autoridades y de su remoción". Constatando además que el Proyecto contiene normativa especial respecto del nombramiento, duración y causales de remoción respecto de la autoridad máxima de la Agencia.

Esta idea ya había sido adoptada por la doctrina nacional, estableciéndose la necesidad imperiosa de que en nuestro sistema jurídico se "implemente una autoridad de control, independiente y especializada en materia de protección de datos personales, investida de potestades de fiscalización, coerción y, por sobre todo, prevención, pues la actual legislación ha perdido eficiencia y eficacia en la resolución de conflictos relacionados con el uso de las nuevas tecnologías"[105].

El hecho de que la Agencia se erija como una entidad independiente y especializada no es una cuestión baladí, puesto que los órganos garantes de derechos que son establecidos como instituciones especializadas e imparciales garantizan el ejercicio el ejercicio autónomo de sus funciones y la protección de los derechos a los que sus atribuciones hacen referencia de forma imparcial y eficaz. Lo anterior es importante ya que uno de los aspectos críticos de este tipo de órganos es que gocen de la suficiente autonomía para que cuenten con los instrumentos necesarios para vencer los obstáculos y resistencias que puedan tener las personas en la protección de sus derechos.

La creación de estos organismos independientes y especializados se encuentra justificada en la necesidad de contar con órganos que entreguen una completa, eficaz y eficiente protección a los derechos de los ciudadanos dentro de un sistema democrático. Por lo tanto, es vital que la Agencia mantenga la naturaleza jurídica que el proyecto modificatorio de la Ley N°19.628 le ha consagrado, ya que solo a través de un órgano con tales características podremos adecuar nuestro sistema a los estándares internacionales exigidos.

III.3.- PATRIMONIO DE LA AGENCIA

A este respecto se ha indicado que la "aspiración de una autoridad de control que ejerza sus funciones independientemente parece mellada por la disponibilidad relativa de recursos para satisfacer su cometido. En ese punto, la problemática central gira en torno a la

[105] HERRERA, P. El derecho a la vida privada y las redes sociales en Chile. Op. Cit. p. 106.

disponibilidad de recursos suficientes y no afectos a los recortes presupuestarios propios de las oscilantes políticas gubernamentales" [106].

Sobre el particular, por ejemplo, "la legislación francesa se ocupa expresamente del régimen presupuestario de la Comisión, si bien ciñe sus créditos a cuenta del presupuesto del Ministerio de Justicia. Además, admite el cobro de tasas por los servicios que resulten de trámites previos al funcionamiento de tratamientos automatizados de informaciones nominativas"[107].

Ahora bien, este es un tema que se encuentra expresamente tratado dentro del Proyecto (en su versión original) en el artículo 36. En dicho artículo se señala que el patrimonio de la Agencia estará establecido, en primer lugar, por el aporte que se contemple de forma anual dentro de la Ley de Presupuestos de la Nación. En segundo lugar, se menciona que también se encontrará conformado por los bienes muebles e inmuebles transferidos o adquiridos por cualquier título, así como también los frutos que de ellos se perciban.

Además, se contempla que el patrimonio de la Agencia pueda ser confeccionado en consideración de las posibles donaciones que la institución acepte, librando a dichas donaciones de la insinuación judicial del artículo 1401 del Código Civil[108]. Esta consideración es importante para poder librar a las donaciones que pueda recibir la agencia de trámites que desincentiven a los posibles donantes en vista de los costos y tiempos asociados a llevar a cabo el trámite de insinuación judicial.

Adicionalmente, el artículo 36 indica que compondrán el patrimonio de la Agencia todas aquellas herencias y legados que dicho órgano acepte, aceptación que siempre deberá ser realizada con beneficio de inventario. Las asignaciones realizadas a la Agencia, a título de herencia o legado, estarán por disposición expresa de la norma exentas de toda clase de impuestos y de todo gravamen o pago que las pudiese afectar de acuerdo a otros cuerpos normativos.

---

[106] CERDA, A. La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales. Universidad de Chile, Facultad de Derecho, 2003. p.190. [En Línea]: http://repositorio.uchile.cl/handle/2250/106762 [consulta: 20 de noviembre 2021].
[107] Idem. p. 190.
[108] Art. 1401 CC. *"La donación entre vivos que no se insinuare, sólo tendrá efecto hasta el valor de dos centavos, y será nula en el exceso. Se entiende por insinuación la autorización de juez competente, solicitada por el donante o donatario. El juez autorizará las donaciones en que no se contravenga a ninguna disposición legal".*

Por otra parte, compondrán también el patrimonio de la Agencia los aportes de cooperación internacional y, en general, todos los demás aportes o recursos que por ley se otorguen a la Agencia de Protección de Datos Personales[109].

Finalmente, una cuestión relevante en torno al patrimonio de la Agencia es que, "al iniciarse el estudio de este precepto, el Presidente de la Comisión, Honorable Senador señor Harboe, se mostró partidario de que un porcentaje de las multas que se apliquen se destinen a la Agencia. Lo anterior con el objetivo de crear un órgano con capacidad efectiva y que pueda llevar a cabo un buen trabajo"[110]. Esta idea fue apoyada por el asesor del Ministerio de Hacienda, señor Godoy, quien sostuvo que recientemente se aprobó una experiencia en la reforma laboral, en que las multas por infracción a los derechos colectivos del trabajo iban a un fondo destinado a programas de capacitación de actores sociales[111].

Sin embargo, es observable que la consignación de un porcentaje de las multas, como parte del patrimonio de la Agencia, no se no se estableció, cuestión que parece acertada, toda vez que un mecanismo elaborado en dicho sentido puede generar incentivos perversos para la autoridad de control, la cual puede ver desvirtuadas sus funciones en favor de obtener mayor recaudación de dinero a través de la imposición excesiva e infundada de multas; la implementación de este sistema de recaudación requiere del desarrollo de mecanismos que eviten los incentivos negativos que conlleva.

III.4.- DIRECTOR O DIRECTORA

III.4.1.- Nombramiento.

Según versa el artículo 33 original del proyecto modificatorio, la dirección y administración superior de la Agencia de Protección de Datos Personales estará a cargo de un Director o Directora, quien será el jefe superior del Servicio. El proyecto da cuenta, en sus disposiciones transitorias, del establecimiento de un plazo de 60 días, contados a partir de la publicación de la ley, dentro del cual deberá convocarse a un concurso público con el fin de poder nombrar al primer Director o Directora de la Agencia de Protección de Datos Personales. Dicho Director o Directora deberá ser designado por el Presidente de la República, conforme

[109] La referencia a los aportes o recursos otorgados por ley es una modificación incluida por la Comisión en su primer informe.
[110] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Op. Cit. p. 480.
[111] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Idem. p.480.

al Sistema de Alta Dirección Pública regulado en el título VI de la ley N° 19.882, afecto al primer nivel jerárquico, y con acuerdo del Senado adoptado por la mayoría absoluta de sus miembros en ejercicio[112].

Es importante destacar que existen dos puntos que "tienden a conformar la independencia de la autoridad de control y se vinculan con su nombramiento, estos son, de un lado, los requisitos que debe satisfacer quien es designado y, por otro lado, el sistema mismo mediante el cual se concluye su nominación.

Respecto de los requisitos que debe cumplir la autoridad de control, los Principios adoptados por las Naciones Unidas en la materia abogan porque la autoridad ofrezca garantía de competencia técnica; otro tanto hace la legislación argentina, que exige que el Director de la entidad de control sea se seleccionado entre personas con antecedentes en la materia."[113]

Particularmente, "cuando la configuración de la autoridad de control reviste un carácter individual, a efectos de resguardar la independencia del mismo se prevé mecanismos de designación conjunta, en que concurren diversos poderes del Estado. Es el caso de Director de la Dirección Nacional de Protección de Datos de la Argentina, quien es designado por el Poder Ejecutivo con acuerdo del Senado de la Nación."[114]

Haciendo eco de lo anterior la Comisión estableció, en su primer informe, una modificación al artículo 33 sobre la designación del Director o Directora, agregando un nuevo inciso en el cual se sostiene que "el Presidente de la República deberá proponer esta designación sesenta días antes de la expiración del plazo de duración del Director saliente. El Senado dispondrá de un término de treinta días corridos para aceptar o rechazar la propuesta. En caso de que no se pronuncie dentro de este plazo se entenderá aceptada la proposición del Presidente de la República. Si el Senado rechaza la proposición del Presidente de la República se deberá repetir el procedimiento hasta que se apruebe o acepte una designación. Otorgada esa aprobación o aceptación, según corresponda, el Presidente de la República, por intermedio del Ministerio de Hacienda, expedirá el decreto supremo de nombramiento del Director de la Agencia de Protección de Datos Personales"[115].

[112] La sujeción de la designación del Director o Directora al acuerdo del Senado es una modificación al Proyecto que fue introducida por la Comisión de Constitución, Legislación, Justicia y Reglamento, según consta en la página 614 del primer informe elaborado por dicha Comisión.
[113] CERDA, A. Op. Cit. p.183.
[114] CERDA, A. Idem. p. 185.
[115] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Op. Cit. p.614.

La idea de que interviniese otro poder del Estado en la designación del Director o Directora fue un tema controversial dentro de la Comisión, por ejemplo, el Senador Quinteros señaló que el hecho de terminar con el sistema binominal dentro de nuestro ordenamiento podría implicar que los nombramiento se alargaran de forma innecesaria, cuestión que solo podría ser revertida si es que se consignaba un quórum necesario para evitar la paralización del nombramiento. En dicho sentido también se manifestó el asesor del Ministerio de Hacienda don Roberto Godoy, quien sostuvo que incorporar a un órgano esencialmente político, como lo es el Senado, desvirtuaría la naturaleza técnica del órgano que se pretende crear[116].

Sin embargo, las posiciones a favor terminaron por dominar en la discusión dentro de la Comisión, ejemplo de esto es que el Presidente de la Comisión (Senador Harboe) señaló que era importante la participación, en la elección del director o Directora de la Agencia, de otro poder del Estado ya que esto permitiría dotar de la suficiente autonomía a la Agencia misma. Además, señaló, como contrargumento a lo expresado por el señor Godoy, que la Cámara alta ya participa de nombramiento de autoridades que no tienen el carácter de políticas como es el caso de los Ministros de la Corte Suprema, por lo tanto, es factible su participación en la designación de cargos dentro de organismos de carácter técnico[117].

Finalmente, se señala en el proyecto modificatorio que es facultativo del Presidente de la República el hecho de nombrar al Director o Directora de la Agencia de Protección de Datos Personales antes de la fecha en que ésta inicie sus actividades para efectos de la instalación de la misma. Por su parte, en tanto la Agencia no inicie sus actividades, la remuneración del Director se financiará con cargo a lo que se disponga en la correspondiente Partida del Presupuesto del Ministerio de Hacienda.

III.4.2.- Duración del cargo

Una cuestión de relevante significancia, agregada por la Comisión, es la estipulación de un período de 5 años para el ejercicio del cargo de Director o Directora de la Agencia, período que podrá ser renovado por una sola vez.

Este tema no revistió discusión dentro de la Comisión, siendo destacable solo lo señalado por parte del Presidente de la comisión, el Senador Harboe, en torno a que la

[116] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Idem. pp. 457-458.
[117] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Idem. pp. 458-459.

permanencia por un período de 5 años en el cargo permitiría que éste no coincida con el ciclo político de elecciones de nuestro país[118]. Cuestión que resulta relevante, y de la mayor sensatez, si lo que se pretende por parte del legislador es dotar de autonomía al órgano supervisor.

III.4.3.- Requisitos para ser nombrado Director o Directora

Como se señaló con anterioridad, el establecimiento de requisitos para el nombramiento del cargo de Director o Directora dentro de una institución revisten importancia de cara a la autonomía que dicho órgano pueda tener dentro de un sistema jurídico. Lamentablemente, los requisitos para poder desempeñar el cargo de Director o Directora de la Agencia no fue un tema que estuviera tratado en el proyecto modificatorio original, sino que fue un añadido posterior realizado por parte de la Comisión. De esta forma, se agregó en el artículo 33 del Proyecto cuatro requisitos que deben ser satisfechos por quienes sean propuestos, por parte del Presidente de la República, al cargo de Director o Directora de la Agencia.

En primer lugar, se señala que la persona postulada al cargo debe cumplir con los requisitos generales para ingresar a la Administración Pública. Dichos requisitos se encuentran consagrados en el artículo 12 de la Ley N°18.834 sobre Estatuto Administrativo[119], artículo en el cual se señala que para ingresar a la Administración Pública se requiere: a) Ser ciudadano[120]; b) Haber cumplido con la ley de reclutamiento y movilización, cuando fuere procedente; c) Tener salud compatible con el desempeño del cargo; d) Haber aprobado la educación básica y poseer el nivel educacional o título profesional o técnico que por la naturaleza del empleo exija la ley; e) No haber cesado en un cargo público como consecuencia de haber obtenido una calificación deficiente, o por medida disciplinaria, salvo que hayan transcurrido más de cinco años desde la fecha de expiración de funciones, y f) No estar

[118] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Idem. p. 457.
[119] Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=236392
[120] La norma señala que no obstante el requisito de ciudadanía "en casos de excepción determinados por la autoridad llamada a hacer el nombramiento, podrá designarse en empleos a contrata a extranjeros que posean conocimientos científicos o de carácter especial. Los respectivos decretos o resoluciones de la autoridad deberán ser fundados, especificándose claramente la especialidad que se requiere para el empleo y acompañándose el certificado o título del postulante. En todo caso, en igualdad de condiciones, se preferirá a los chilenos".

inhabilitado para el ejercicio de funciones o cargos públicos, ni hallarse condenado por delito que tenga asignada pena de crimen o simple delito[121].

Como segundo requisito se señala que el optante deberá tener a lo menos siete años de ejercicio de la profesión, además de contar con reconocido prestigio profesional o académico en el ámbito de la protección de los datos personales. Este requisito revistió una particular discusión en la Comisión debido a que algunos senadores como, por ejemplo, el Senador Larraín se mostraron partidarios de la idea de exigir diez años de ejercicio de la profesión. Sin embargo, esta idea no imperó dentro de la Comisión manteniéndose el plazo de siete años en base a razones como que el plazo de diez años podría significar la afectación de mujeres profesionales que no cuenten con los años de ejercicio solicitados o el ejemplo dado por el CPLT donde se ha evidenciado la presencia de profesionales con menor experiencia que han logrado un buen trabajo respecto de la protección de datos en el ámbito público[122].

Finalmente, como cuarto requisito para el cargo, se señala que la persona deberá acreditar una experiencia laboral relevante en materias relacionadas con las funciones y competencias de la Agencia de Protección de Datos Personales. Este requisito es clave si lo que queremos es tener una Agencia que cumpla de forma eficiente y eficaz las tareas encomendadas por la ley; si la persona designada no tuviere expertiz en el área se generarían problemáticas que dificultarían un sistema de protección efectivo para los derechos de los titulares de datos.

III.4.4.- Funciones y atribuciones.

Por otra parte, el mismo artículo 33 del proyecto, en su versión original, nos menciona las diferentes funciones y atribuciones que posee el Director o Directora que asuma la dirección de la Agencia.

En primer lugar, el artículo nos señala, en su literal a), que es deber del Director o Directora de la Agencia el velar por el respeto, defensa y protección de los derechos y libertades de las personas que son titulares de datos, en particular el derecho a la vida privada,

[121] Se indica que sin perjuicio de aquél requisito, tratándose del acceso a cargos de auxiliares y administrativos, no será impedimento para el ingreso encontrarse condenado por ilícito que tenga asignada pena de simple delito, siempre que no sea de aquellos contemplados en el Título V, Libro II, del Código Penal.
[122] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Op. Cit. pp.462-463.

promoviendo una cultura de información, educación y participación ciudadana de acuerdo con los principios y derechos que se consagran en el proyecto.

En segundo lugar, el literal b), nos menciona que el Director o Directora deberá fiscalizar y supervigilar el tratamiento de los datos personales que realicen las personas naturales y jurídicas, sin distinción respecto a si estas son de naturaleza pública o privada, con el objeto de que cumplan los principios y obligaciones establecidos la ley.

El Director o Directora también tendrá entre sus funciones el asesorar al Ministro o Ministra de Hacienda en el estudio y proposición de las reformas legales aplicables al tratamiento de los datos personales y su protección. Además, deberá realizar labores de interpretación administrativa respecto de las disposiciones legales en materia de protección y tratamiento de datos personales, así como también el dictar las normas e instrucciones generales necesarias para su aplicación y fiscalización[123].

En cuarto lugar, según dispone el literal d) del artículo 33, quien desempeñe el cargo deberá absolver las consultas sobre la aplicación e interpretación de las normas relativas a la protección de datos y su tratamiento que formulen las personas naturales y jurídicas. Además, deberá realizar la planificación de las labores de fiscalización de la Agencia y desarrollar todas las políticas y/o programas que resulten necesarios con el fin de promover la prevención y la autorregulación con miras a la protección de los derechos sobre datos personales que se consagran en la ley[124].

El Director o Directora de la Agencia además deberá asumir la tarea de dirigir, organizar, planificar y coordinar el funcionamiento de la Agencia de Protección de Datos Personales; dictar las órdenes necesarias para una marcha expedita de ésta y supervigilar el cumplimiento de las instrucciones que para dichos fines imparta.

Una de las más importantes atribuciones que poseerá el Director o Directora es la de representar a la Agencia en todos los asuntos que le competan, incluidos los recursos judiciales y los recursos extraordinarios que se interpongan en contra de la Dirección, ya sea con motivo de actuaciones administrativas o jurisdiccionales[125]. La Comisión optó por establecer que, en razón de determinados casos, deberá el Director o Directora actuar en coordinación con el CPLT.

[123] Artículo 33 literales c) y d).
[124] Artículo 33 literal f).
[125] Artículo 33 literal h).

Sumado a lo anteriormente señalado, el Proyecto dispone que el Director o Directora nombrado deberá presentar al Ministerio de Hacienda, antes del 31 de marzo de cada año, una memoria anual sobre la marcha de la Agencia de Protección de Datos Personales. Así como también deberá proponer al Presidente de la República, a través del Ministerio de Hacienda, las medidas que a su juicio convenga adoptar para la mejor marcha de la Agencia, desarrollando todas las iniciativas tendientes a conseguir un desarrollo óptimo de las facultades de la institución[126].

Finalmente, cabe hacer presente que la Comisión optó por agregar una función relevante para el cargo de Director o Directora[127], cual es la función de promover la participación ciudadana en las materias relacionadas con la protección y el tratamiento de los datos personales, observando siempre los principios y derechos que establece la ley[128]. Permitiendo la posibilidad de que el Director o Directora pueda delegar sus funciones y atribuciones en funcionarios de su dependencia, de conformidad a la ley.

Esta última función enunciada resulta de total relevancia en el mundo digital que hoy observamos, con la participación ciudadana las personas podrán interiorizarse y adquirir mayor conocimiento de sus derechos respecto de sus datos personales, lo cual implicará una mejora en el cuidado ejercido de cara a la recolección y tratamiento por parte de quienes recopilan los datos de los titulares.

III.4.5.- Incompatibilidades e Inhabilidades

Sobre este punto, la doctrina ha señalado que para "reforzar la independencia del órgano, es usual que las leyes contemplen la sujeción del mismo a ciertas inhabilidad coexistentes a su desempeño e inclusive sobrevivientes a él, específicas de su función o aquellas genéricas previstas en la legislación interna.

Así, por ejemplo, la legislación argentina, junto con disponer la "dedicación exclusiva" de quien detente el cargo de Director de la Dirección Nacional de Protección de Datos, le extiende las incompatibilidades fijadas por la ley para los funcionarios públicos."[129]

[126] Artículo 33 literales i) y j).
[127] Se puede apreciar en el primer informe de la Comisión la decisión de establecer las funciones y atribuciones en un artículo separado, como lo es el art.33 bis, respecto de las materias de nombramiento y requisitos para el cargo que se mantienen reguladas en el art.33 del Proyecto.
[128] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Op. Cit. p.615.
[129] CERDA, A. Op. Cit. p. 187.

Referente a lo anterior, según dispone el artículo 34 del Proyecto, se evidencia que el desempeño del cargo de Director o Directora exige dedicación exclusiva y es incompatible con el desempeño de todo otro cargo o servicio que se preste en el sector privado (con independencia de si dicho cargo del sector privado es remunerado o no).

Asimismo, el cargo de Director o Directora de la Agencia es incompatible con todo otro empleo o servicio retribuido con fondos fiscales o municipales, y con las funciones, remuneradas o no, de consejero, director o trabajador de instituciones públicas, organismos autónomos nacionales o extranjeros, empresas del Estado y, en general, de todo servicio público creado por ley, como, asimismo, de empresas, sociedades o entidades públicas o privadas en que el Estado, sus empresas, sociedades o instituciones centralizadas o descentralizadas, tengan aportes de capital mayoritario o en igual proporción o en las mismas condiciones, representación o participación. También es incompatible con cualquier otro servicio o empleo remunerado o gratuito en otros poderes del Estado.

Resulta relevante destacar que el cargo de Director o Directora sí resulta compatible con el desempeño de cargos docentes en instituciones públicas o privadas reconocidas por el Estado, siempre y cuando dicha labor se desempeñe hasta por un máximo de doce horas semanales. Del mismo modo, se señala que el Director o Directora podrá desempeñarse en corporaciones o fundaciones (públicas o privadas, nacionales o extranjeras) siempre que en ellas no perciba remuneración alguna y su desempeño no sea incompatible con sus funciones.

Por otra parte, nos señala el artículo 34 que respecto del cónyuge o conviviente civil del Director o Directora y sus parientes (hasta el segundo grado de consanguinidad inclusive) existe la prohibición de ejercer el cargo de director o directora ni tener participación en la propiedad de una empresa cuyo objeto o giro comercial verse sobre recolección, tratamiento o comunicación de datos personales.

Finalmente, la Comisión decidió modificar el artículo 34 del proyecto incorporando a este un último inciso que da cuenta de las inhabilidades para el cargo de Director o Directora. De esta forma se señala que no podrá ser designado Director o Directora de la Agencia la persona que hubiere sido condenada por delito que merezca pena aflictiva o inhabilitación perpetua para desempeñar cargos u oficios públicos, por delitos de prevaricación, cohecho y aquéllos cometidos en ejercicio de la función pública, delitos tributarios y los delitos contra la fe pública; tampoco podrá ejercer el cargo la persona que tuviere dependencia de sustancias o drogas estupefacientes o sicotrópicas ilegales, a menos que justifique su consumo por un

tratamiento médico[130]; o la persona que haya sido sancionada, dentro de los últimos tres años, por infracción gravísima a las normas que regulan el tratamiento de los datos personales y su protección[131].

III.4.6.- Causales de cese en el cargo

Una cuestión importante en torno a este tema es que "la eventualidad de que la autoridad de control fuese objeto de la remoción de su cargo como represalia del desempeño de sus funciones ciertamente representaría una seria lesión para la pretendida independencia de la misma; es por ello que la generalidad de las legislaciones revisadas aseguran cierta inamovilidad a quien hace las veces de autoridad de control, lo cual se logra con jugando un plazo determinado de duración en el cargo con la prevención de ciertos eventos, de preferencia excepcionales, que dan lugar a la terminación anticipada de su contenido.

Así, por ejemplo, en el caso de Francia, los miembros de la Comisión son designados para cumplir su cometido en ella por el plazo de cinco años o, excepcionalmente, el tiempo que durare su mandato, y salvo en el caso de dimisión, sólo pueden ser cesados en sus funciones cuando concurre un impedimento apreciado por la propia Comisión, de acuerdo a las condiciones definidas por la misma."[132]

Cabe precisar que la cuestión entorno a las causales que implican el cese de las funciones del Director o Directora de la Agencia no fue tratada en el texto original del proyecto modificatorio, sino que fue una invención realizada por la Comisión incluida dentro del artículo 33 como se da cuenta en el primer informe elaborado. Así, la Comisión decidió establecer 5 causales de cese o remoción del cargo.

En primer lugar, bajo el literal a), se menciona que cesa en sus funciones el Director o Directora que haya cumplido el período legal de su designación. En segundo lugar, literal b), se menciona que la renuncia voluntaria del Director aceptada por el Presidente de la república también será considerada una causal de cese. Por su parte, el literal c) indica que cesará en

[130] Esta idea dice relación con lo señalado por la señora Piedrabuena, quien actuó dentro de la Comisión como asesora del Ministerio de Economía, en cuanto a que las sustancias psicotrópicas que pueden ser recetadas por un médico, deben ser legales. En: COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Op. Cit. p. 474.
[131] Termina el artículo señalando que en todo lo no expresamente regulado en dicha disposición se regirá por las normas del párrafo 2° del Título III (sobre las inhabilidades e incompatibilidades administrativas) de la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.
[132] CERDA, A. Op. Cit. pp. 188-189.

su puesto el Director que se vea afecto a alguna de las causales de inhabilidad o incompatibilidad establecidas en el artículo 34 del proyecto mencionadas en el punto anterior de este trabajo.

Finalmente, se da cuenta en los literales d) y e) de dos causales especiales como lo son la incapacidad física o síquica para el desempeño del cargo, y el incumplimiento grave de las funciones y deberes que el cargo exige. La particularidad de estas causales viene dada porque se establece que la remoción fundada en aquellas "será dispuesta por la Corte Suprema a requerimiento del Presidente de la República o de la Cámara de Diputados mediante acuerdo adoptado por simple mayoría. La Corte Suprema conocerá del asunto en pleno especialmente convocado al efecto y para acordar la remoción deberá reunir el voto conforme de la mayoría de sus miembros en ejercicio"[133].

III.4.- FUNCIONES Y ATRIBUCIONES DE LA AGENCIA

El Proyecto contiene, en su artículo 31[134], un catálogo de facultades generales conferidas a la Agencia, las cuales nos permitirán establecer los lineamientos generales sobre los cuales podrá actuar nuestra autoridad de control. Dichas facultades son establecidas en el Proyecto en miras a mejorar nuestro sistema de protección de datos personales, permitiendo acercar a nuestro país a los estándares internacionales imperantes.

III.4.1.- Proposición e interpretación normativa.

En primer lugar, se menciona como facultad de la Agencia el poder aplicar e interpretar administrativamente las disposiciones legales y reglamentarias cuyo cumplimiento le corresponde vigilar, así como también el impartir instrucciones de carácter general a las personas naturales o jurídicas que realicen tratamiento de datos personales. Dichas

[133] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Op. Cit. p.614.
[134] Cabe hacer presente que dicha norma sufrió cambios durante la discusión y análisis del Proyecto realizado por la Comisión, por tanto, las facultades y atribuciones señaladas corresponden a las resultantes de dichas discusiones y no con las señaladas en el artículo original del Proyecto.

instrucciones generales que dicte la Agencia deberán ser sometidas a una consulta pública efectuada (a través de su página web institucional) de forma previa a su dictación[135].

En torno a esta facultad, el asesor del Ministerio de Hacienda, don Roberto Godoy, señaló que "responde a la atribución más genérica de la Agencia y dice relación con la facultad de poder aplicar e interpretar administrativamente la ley en materia de protección y tratamiento de datos personales. Asimismo, se le otorga la potestad de dictar instrucciones de carácter general, con el objeto de lograr la aplicación de la ley"[136]. Así como también destacó que el hecho de someter a consulta pública las instrucciones efectuadas por la Agencia no es sino una adecuación de nuestro ordenamiento jurídico a las exigencias que nos presenta la OCDE.

Además, la Agencia deberá proponer al Presidente de la República 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[137]. Con esta facultad lo que la Comisión pretendió fue permitir a la Agencia tomar un rol protagónico en la creación de normas relativas a la protección de datos personales debido a su especialización, pero evitando que ésta se convierta en un órgano que pueda presentar, directamente, proyectos de ley al Congreso Nacional; por este motivo es que se somete a la Agencia a la supervigilancia del Presidente de la República a través de esta regla de proposición normativa[138].

Las facultades en torno a la normativa de protección de datos personales contemplará además la funciones de prestar asistencia técnica, cuando le sea requerida, a diferentes órganos de nuestro ordenamiento como, por ejemplo, el Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el Banco Central, el Servicio Electoral, la Justicia Electoral y/o los demás tribunales especiales creados por ley, siempre que dicha asistencia técnica diga relación con la dictación y ejecución de las políticas y normas internas de estos organismos sobre el tratamiento y la protección de los datos personales[139]. Así como también deberá colaborar con los órganos públicos en el

[135] Dicha facultad se encuentra contenida en el artículo 33 literal a) de las modificaciones realizadas por la Comisión. El art. 31 del Proyecto en su forma original disponía: "*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, salvo aquellos tratamientos de datos regidos por leyes especiales y sujetos a la potestad normativa de otro órgano público. Las instrucciones y normas generales que dicte la Agencia de Protección de Datos Personales deberán ser emitidas previa consulta pública efectuada a través de la página web institucional*".
[136] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Op. Cit. p.436.
[137] Artículo 31 f), modificado por la Comisión.
[138] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Op. Cit. pp. 442-443.
[139] Artículo 31 i), modificado por la Comisión.

diseño e implementación de políticas, programas y acciones destinadas a velar por la protección de los datos personales y su correcto tratamiento[140].

Es importante señalar que la Agencia tendrá que relacionarse, en el ejercicio de sus funciones propositivas e interpretativas respecto de normativa de protección de datos personales, con los organismos públicos y demás órganos del Estado que resulte necesario[141]. En vistas de estas posibles relaciones es que se decidió establecer dentro del Proyecto, por ejemplo, un deber de coordinación regulatoria entre la Agencia y el CPLT[142]. Así, de acuerdo con las modificaciones realizadas por la Comisión, cuando la Agencia deba dictar una instrucción general que tenga efectos en los ámbitos de competencia del CPLT, deberá remitir a este último todos los antecedentes necesarios, y requerirá de éste un informe para efectos de evitar o precaver conflictos de normas y asegurar la coordinación, cooperación y colaboración entre ambos órganos[143]. Finalmente, dispone dicho precepto que cuando la instrucción general afecte a cualquier otro órgano de la Administración del Estado, se aplicará lo dispuesto en el artículo 37 bis de la ley N° 19.880.

III.4.2.- Facultad de promoción y protección de los derechos sobre datos personales

La idea general en torno a que la Agencia deberá velar por la protección y promoción de los derechos sobre datos personales la encontramos en el inciso final del artículo 10 del Proyecto, en el cual se nos señala que la Agencia deberá velar por el efectivo ejercicio y cumplimiento de los derechos que la ley reconoce y confiere a los titulares de datos.

Respecto de este punto cabe destacar la estipulación expresa en favor de la Agencia para que ésta pueda desarrollar programas, proyectos y acciones de difusión, educación, promoción e información dirigidos a la ciudadanía y a los responsables de datos, en relación al respeto y protección del derecho a la vida privada y a la protección de los datos

[140] Artículo 31 j), modificado por la Comisión.
[141] Artículo 31 g), modificado por la Comisión.
[142] Artículo 32.
[143] La norma señala además que el CPLT deberá evacuar el informe solicitado dentro del plazo de treinta días corridos, los cuales se computarán desde la fecha en que hubiere recibido el requerimiento antes señalado. La normativa señala que la Agencia deberá valorar el contenido de la opinión del CPLT expresándolo en la motivación de la instrucción que dicte. Lo anterior en base a lo dispuesto en el artículo 41 de la ley N° 19.880.
A su vez, cuando el Consejo para la Transparencia deba dictar una instrucción general que tenga efectos en los ámbitos de competencia de la Agencia de Protección de Datos Personales, de acuerdo a las funciones y atribuciones señaladas en esta ley, el Consejo remitirá los antecedentes y requerirá informe a la Agencia de Protección de Datos Personales, quien deberá evacuarlo en el plazo de treinta días corridos, contado desde la fecha en que hubiere recibido el requerimiento. El Consejo valorará el contenido de la opinión de la Agencia de Protección de Datos Personales expresándolo en la motivación de la instrucción general que dicte al efecto.

personales[144]. Para esto la Agencia podrá participar, recibir cooperación y colaborar con organismos internacionales en materias propias de su competencia[145].

Lo antes señalado no es una cuestión que resulte irrelevante, por el contrario, dichos mecanismos de colaboración y participación serán de suma importancia para poder conocer, comprender y aplicar, en nuestro ordenamiento, políticas innovadoras en materia de protección de datos personales que permitan acercar a nuestro país a los más altos estándares exigidos tanto por la OCDE como por la Unión Europea.

Además, para efectos de la promoción y protección de los derechos de los titulares de datos la Agencia podrá celebrar convenios o memorandos de entendimiento con organismos nacionales, internacionales o extranjeros, sean estos públicos o privados y desarrollar programas de asistencia técnica[146]. Cuestión que gira en el mismo sentido que lo expresado en el párrafo anterior, es decir, poder conocer intentar replicar normativa que nos permita acercarnos a los estándares internacionales y contar con un sistema más robusto de protección de datos personales.

III.4.3.- Facultad de fiscalización y sanción.

Siempre que se aborda un órgano de autoridad las cuestiones centrales giran en torno a las facultades de fiscalización y/o sanción que el órgano en cuestión posea. Así, se señala en el Proyecto que es facultad de la autoridad de control el fiscalizar y velar por el cumplimiento de los principios, derechos y obligaciones establecidos la ley, estableciendo que, para dichos efectos, podrá solicitar la entrega de cualquier documento, libro o antecedente que se estime necesario[147]. Es importante destacar que la facultad de requerir documentación se entiende exclusivamente circunscrita a la existencia de un proceso de fiscalización o de investigación y no es una facultad que se pueda ejercer de forma amplia por la Agencia; tal como se destaca por parte del presidente de la Comisión, dicho marco viene dado por la expresión “para efectos de fiscalización”[148].

[144] Artículo 31 h), modificado por la Comisión.
[145] Artículo 31 l), modificado por la Comisión.
[146] Artículo 31 k), modificado por la Comisión.
[147] Dicha facultad fue incluida por la Comisión en el literal b) del Artículo 31 del Proyecto.
[148] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Op. Cit. p.438.

En segundo lugar, se dispone que la Agencia deberá resolver las solicitudes y reclamaciones que formulen los titulares en contra de los responsables de datos[149], así como también deberá investigar y determinar las infracciones en que incurran dichos responsables, estableciendo las sanciones que correspondan una vez terminados los procedimientos llevados a cabo para tales fines; esta cuestión no es sino una manifestación de la potestad investigadora y sancionatoria que revestirá la Agencia.

Para cumplir con dichos propósitos la Agencia podrá citar a declarar, entre otros, al titular, a los representantes legales, administradores, asesores y dependientes del responsable de datos, así como a toda persona que haya tenido participación o conocimiento respecto de algún hecho que sea relevante para resolver un procedimiento sancionatorio. Asimismo, podrá tomar las declaraciones respectivas por otros medios que aseguren su Fidelidad[150].

Lo anterior es expresión de "una facultad genérica que corresponde normalmente a los organismos que cumplen labores de fiscalización. Ésta consiste en investigar y determinar aquellos hechos que constituyen una infracción a la ley. Agregó que se le otorgan a la Agencia facultades necesarias para cumplir las labores de investigación"[151-152].

III.4.3.1.- Fiscalización en materia de transferencia internacional de datos personales

En materia de fiscalización de transferencias internacionales de datos personales la Comisión optó por modificar sustantivamente el Título V del Proyecto que se abocaba al tratamiento de este tema. En tal sentido, las facultades de la Agencia quedaron comprendidas en los artículos 28 y 29 del Proyecto.

En base a estos artículos la Agencia deberá determinar fundadamente el listado de países que poseen niveles adecuados de protección de datos, esto con el fin de poder brindar licitud a las operaciones de transferencia internacional de datos que con dichos países se pretenda realizar.

[149] Artículo 31 c), modificado por la Comisión.
[150] Artículo 31 d), modificado por la Comisión.
[151] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Op. Cit. p.439.
[152] Cabe mencionar que respecto de estas facultades la Agencia podrá adoptar las medidas preventivas o correctivas que disponga la ley.

En primer lugar, se menciona que un país será adecuado cuando su ordenamiento contemple el establecimientos de principios que rijan el tratamiento de datos personales. En segundo lugar, el país será adecuado cuando existan en su ordenamiento jurídico normas que reconozcan y garanticen los derechos de los titulares de datos, así como también se consagre la existencia de una autoridad pública jurisdiccional o administrativa de control o tutela. Además, se tendrá en consideración la imposición de obligaciones de información y seguridad a los responsables del tratamiento de datos y la existencia de responsabilidades en caso de que se cometan infracciones a la normativa de protección de datos personales.

El Proyecto indica que, en caso de no verificarse las circunstancias del artículo 27[153], la Agencia podrá autorizar, mediante resolución fundada, la transferencia internacional de datos siempre que el transmisor y el receptor de los datos otorguen las garantías adecuadas en relación con la protección de los derechos de las personas que son titulares de estos datos y la seguridad de la información transferida. Así mismo, la Agencia, con el fin de poder salvaguardar los derechos de los titulares de datos, podrá imponer condiciones previas para que se verifique la transferencia.

Finalmente, se indica que será facultativo de la Agencia el fiscalizar las operaciones de transferencia de datos, pudiendo formular las recomendaciones que estime necesarias para tales efectos, adoptar medidas conservativas y, en casos calificados, suspender temporalmente el envío de datos.

III.4.4.- Facultad consultiva

Dentro de esta facultad se deberá entender comprendida el hecho de que la Agencia podrá resolver las solicitudes o consultas relativas a si una determinada base de datos o conjunto de datos es considerada fuente de acceso público e identificar categorías genéricas que posean esta condición[154].

Un punto relevante en torno a esta facultad es que, dentro de la Comisión, “el abogado analista del Consejo para la Transparencia, señor Alejandro González, estimó que el punto en discusión es fundamental respecto a las competencias que posee el Consejo, en relación al concepto de fuentes de acceso público. Opinó que las controversias que se van a suscitar

[153] Artículo que enumera una serie de situaciones en las cuales se considerarán lícitas las operaciones de transferencia internacional de datos.
[154] Artículo 31 ñ), modificado por la Comisión.

pueden constituir un flanco que puede llegar a judicializarse. Agregó que, al entregar esta competencia, desde el punto de vista administrativo, a la Agencia, se pierde el punto de equilibrio entre las competencias de ambos órganos respecto al concepto de fuente de acceso público, fundamental para resolver eventuales controversias." A raíz de esta puntualización realizada por el abogado González es que el Presidente de la Comisión propuso reemplazar la expresión "controversias" contenida en la propuesta original del ejecutivo por el término "consultas" que se evidencia en la modificación final del Proyecto[155].

III.4.5.- Certificación, registro y supervisión del modelo de prevención de infracciones y reglamento.

El artículo 31 del Proyecto, en relación con el artículo 53 del mismo, continua señalando que será deber de la Agencia el certificar, registrar y supervisar los modelos de prevención de infracciones y los programas de cumplimiento y administrar el Registro Nacional de Cumplimiento y Sanciones[156]. Para tales efectos, la Agencia de Protección de Datos Personales deberá crear un registro público en que consten las entidades que posean una certificación, así como también aquellas cuya certificación haya sido revocada[157].

En torno a radicar esta facultad en la Agencia el asesor del Ministerio de Hacienda señaló que "en el derecho comparado son las empresas auditoras privadas las que certifican los modelos de prevención. Sin embargo, la experiencia a nivel nacional apunta que ello debe ser realizado por el órgano que se crea"[158]. Lo anterior no impide que la Agencia pueda subcontratar a una empresa que realice la labor de certificación, sin embargo, la responsabilidad que se derive de dicha certificación recaerá, en definitiva, sobre la Agencia.

Por su parte, la regulación de dichos modelos se encuentra, dentro del Proyecto, en el Párrafo Sexto ("Del modelo de prevención de infracciones") del Título VII "De las infracciones y sus sanciones, de los procedimientos y de las responsabilidades". En este se menciona que los responsables de datos, personas naturales o jurídicas (de carácter público o privado),

---

155 El literal original propuesto por el ejecutivo disponía: "ñ) Resolver las solicitudes y controversias que se susciten sobre si una determinada base de datos o conjunto de datos es considerada fuente de acceso público e identificar categorías genéricas, clases o tipos de datos, conjuntos de datos o bases de datos que posean esta condición.".
156 Artículo 31 n), modificado por la Comisión.
157 El artículo 53 señala que "un reglamento expedido por el Ministerio de Hacienda y suscrito por el Ministro Secretario General de la Presidencia y por el Ministro de Economía, Fomento y Turismo establecerá los requisitos, modalidades y procedimientos para la implementación, certificación, registro y supervisión de los modelos de prevención de infracciones y los programas de cumplimiento".
158 COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Op. Cit. p.558.

deberán[159] adoptar mecanismos para prevenir la comisión de las infracciones que señalan los artículos 38 bis, 38 ter y 38 quater del Proyecto[160]. Adicionalmente, los responsables de datos podrán voluntariamente adoptar modelos de prevención de infracciones que deberán contener la designación de un encargado de prevención o delegado de protección de datos personales y sus facultades[161], así como también el establecimiento de un programa de cumplimiento[162].

Los responsables de datos que incurran en alguna de las infracciones previstas en los artículos antes señalados podrán atenuar su responsabilidad solo si acreditan haber cumplido fehacientemente sus deberes de dirección y supervisión para la protección de los datos personales bajo su responsabilidad o tratamiento. El cumplimiento fehaciente de los deberes mencionados solo se entenderá satisfecho cuando el responsable de datos cuente con un certificado emitido por la Agencia, con anterioridad a la infracción, en el que conste la adopción e implementación de un modelo de organización, administración y supervisión para prevenir infracciones[163]. Con esto se logra dotar a nuestro sistema de protección de datos personales de un modelo de responsabilidad objetivo en conformidad a las exigencias internacionales.

Finalmente, cabe señalar que los certificados expedidos por la Agencia tendrán una vigencia de tres años, sin perjuicio que la autoridad pueda dejarlos sin efecto antes de tiempo en base a las causales señaladas en los literales del artículo 55 del Proyecto, así como también podrá revocar la certificación si el responsable de datos no da cumplimiento a las exigencias mencionadas en la ley[164].

---

[159] Al analizar el artículo 52 del Proyecto la Comisión se descantó por reemplazar el término "podrán" por la palabra "deberán" en atención a que el carácter facultativo de la disposición implicaría restar fuerza al modelo en cuestión.
[160] Artículo 52.
[161] El responsable de datos debe disponer que el encargado de prevención cuente con los medios y facultades suficientes para el desempeño de sus funciones. Señala además el artículo 52 que será de cargo del responsable de datos el otorgar al encargado de prevención los recursos materiales necesarios para realizar adecuadamente sus labores.
[162] Dicho programa deberá contener, de acuerdo al artículo 52, lo siguiente:
"1. La identificación del tipo de información que la entidad trata, el ámbito territorial en que opera, la categoría, clase o tipos de datos o bases de datos que administra, la caracterización de los titulares de datos y el o los lugares donde residen estos últimos.
2. La identificación de las actividades o procesos de la entidad, sean habituales o esporádicos, en cuyo contexto se genere o incremente el riesgo de comisión de las infracciones señaladas en los artículos 38 bis, 38 ter y 38 quater.
3. El establecimiento de protocolos, reglas y procedimientos específicos que permitan a las personas que intervengan en las actividades o procesos indicados en la letra anterior, programar y ejecutar sus tareas o labores de una manera que prevenga la comisión de las referidas infracciones.
4. Mecanismos de reporte hacia las autoridades para el caso de contravenir lo dispuesto en la presente ley.
5. La existencia de sanciones administrativas internas, así como de procedimientos de denuncia o persecución de responsabilidades de las personas que incumplan el sistema de prevención de infracciones.".
[163] Artículo 54.
[164] El responsable de datos podrá volver a solicitar el certificado cuando haya acreditado fehacientemente que la causal que dio origen a la revocación ha sido subsanada.

III.4.6.- Representación judicial de sus intereses

Por último, es relevante señalar que la Agencia podrá asumir o solicitar al Consejo de Defensa del Estado, en conformidad a la ley, la representación judicial de sus intereses[165].

Dentro de la Comisión, al abordar este tema en particular, "el asesor del Honorable Senador Larraín, señor Olmedo, sostuvo que la intervención del Consejo de Defensa del Estado en procedimientos de reclamación, que eventualmente se interpongan en contra de las decisiones de la Agencia, puede generar una afectación a la igualdad procesal, respecto al sector privado. Consideró que la Agencia debiese tener su propio sistema de defensa judicial, puesto que el mencionado Consejo está dotado de atribuciones específicas para velar por los intereses del Fisco"[166].

Este argumento fue rebatido por el asesor del Ministerio de Hacienda, señor Godoy, quien declaró que no compartía que se produjese tal "afectación al principio de la igualdad procesal entre las partes, en virtud de la representación del Consejo de Defensa del Estado. Añadió que este último tiene diversas facultades de representación de los intereses del Estado, y en el caso planteado consistiría en asumir la representación de una institución nueva. La razón de haber ocupado la fórmula que se sugiere, es que la Agencia que se crea es eminentemente técnica, sin capacidad de absorber la defensa judicial. Constató que el órgano se situará en la Región Metropolitana y carecerá del despliegue territorial. Por lo tanto, como la función de representación judicial de sus intereses debe ser desarrollado a lo largo del país, se optó porque la defensa jurídica de ella, se realice a través del Consejo de Defensa del Estado"[167]. Finalmente, recordó que existen varias instituciones que son representadas judicialmente por dicho Consejo, utilizando como ejemplo a la Comisión para el Mercado Financiero (CMF), entidad que se encontraría en la misma situación que la Agencia.

Esta idea fue secundada por el asesor del Comité Udi, señor Mery, quien indicó que lo dispuesto en el literal m) del artículo 31 del Proyecto no es sino una mención explícita a la facultad que posee todo organismo público de poder acudir al Consejo de Defensa del Estado[168], por tanto, no sería lógico privar a la Agencia de poder acudir a dicho organismo,

[165] Artículo 31 m), modificado por la Comisión.
[166] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. *Op. Cit.* p.445.
[167] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Ídem. p.445.
[168] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Idem. p.446.

toda vez que es una facultad entregada por el legislador sin ningún tipo de distinción entre los diversos organismos del aparato estatal.

CAPÍTULO IV: PROCEDIMIENTOS ANTE LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES

El Proyecto no solo pretende la conformación de una autoridad especializada en materia de datos personales, sino que se hace cargo de otra deficiencia evidente de nuestro sistema el cual es la falta de mecanismos o procedimientos adecuados para lograr una efectiva y eficaz protección de los derechos de los titulares de datos.

Así, el Proyecto contempla dos tipos de procedimientos: dos de tipo administrativo (tutela de derechos y de infracción de ley) y uno posterior, de tipo judicial (de reclamación). Como se ha mencionado con anterioridad en este trabajo, el establecimiento de un procedimiento o instancia administrativa previa permitirá dotar a nuestros sistema de una mejor herramienta de protección de los derechos de los titulares de datos en comparación con las alternativas contenidas en la actual normativa, la cual es directamente judicial y de escaza aplicación práctica[169].

IV.1.- PROCEDIMIENTOS ADMINISTRATIVOS

IV.1.1.- Procedimiento administrativo de tutela de derechos

Podemos observar en el Proyecto, a partir del artículo 45, la regulación de un primer procedimiento encaminado a la protección de los derechos de titulares de datos. En este procedimiento administrativo de tutela de derechos, que no podrá durar más de seis meses, el titular de datos podrá reclamar ante la Agencia de Protección de Datos Personales cuando un responsable le haya denegado, en forma expresa o tácita, una solicitud en que ejerce cualquiera de los derechos reconocidos y otorgados por la ley[170]. Cabe hacer presente que ante una solicitud de cualquier tipo es la propia entidad (sea pública o privada), en primer lugar, la que debe responder siguiendo, para tales efectos, el procedimiento contemplado en el

[169] VERGARA, M. Chile: comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la agencia de protección de datos personales. Op. Cit. p. 142.
[170] Art. 45.

artículo 11 del Proyecto, y solo en caso de que esta solicitud sea denegada es que el titular de datos podrá recurrir a lo dispuesto en el artículo 45.

Dicha reclamación deberá ser presentada por escrito, dentro del plazo de 15 días contados desde que reciba la respuesta negativa del responsable de datos o haya vencido el plazo que disponía el responsable para responder el requerimiento formulado por el titular. La reclamación deducida deberá singularizar la decisión que pretende impugnar, acompañando para tales efectos todos los antecedentes en que se funda. Además, a petición fundada del titular y sólo en casos justificados, la Agencia podrá suspender el tratamiento de los datos personales que conciernen al titular y que son objeto de la reclamación, debiendo previamente oír al responsable de datos[171].

Por su parte la Agencia, en un plazo de 10 días[172] (contados desde que se ha recibido el reclamo) deberá determinar si éste cumple con los requisitos expresados con anterioridad y así acoger dicha reclamación a tramitación; acogida que sea a tramitación, la Agencia deberá notificar al responsable de datos, quien dispondrá de un plazo de 15 días para responder la reclamación[173], acompañando todos los antecedentes que estime pertinentes[174]. En caso contrario, es decir, en el supuesto de que no se acoja a trámite la reclamación, la resolución de la Agencia deberá ser fundada y notificada al titular[175].

Según dispone el Proyecto, la Agencia de Protección de Datos Personales tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución, así como también podrá convocar a las partes a una audiencia e instarlas a alcanzar un acuerdo; de lograrse el acuerdo correspondiente entre las partes se deberán archivar los antecedentes recolectados durante el procedimiento

Finalmente, la resolución del reclamo dictada por la Agencia de Protección de Datos Personales, mediante la cual se pone término al procedimiento de reclamación, deberá ser debidamente fundada. Por su parte, la resolución de la Agencia de Protección de Datos

---

171 El Artículo 46 h) en su inciso final dispone que "*las reclamaciones y las solicitudes de suspensión del tratamiento formuladas en caso de rechazo de una solicitud de bloqueo temporal, deberán ser resueltas por la Agencia de Protección de Datos Personales en el más breve plazo, sin necesidad de oír previamente a las partes.".*

172 Originalmente el Proyecto contemplaba un plazo de 10 días para tales efectos, pero fue decisión de la Comisión el ampliar el plazo al tiempo señalado.

173 Artículo 46: "d*) Vencido este plazo, haya o no contestado el responsable de los datos y, sólo si existen hechos sustanciales, pertinentes y controvertidos, se podrá abrir un término probatorio de 10 días en el cual las partes pueden hacer valer todos los medios de prueba que estimen convenientes.".*

174 Según dispone el artículo 46 letra c) "*Las notificaciones que se practiquen al responsable se realizarán a la dirección de correo electrónico a que alude la letra c) del artículo 14 ter*.".

175 La notificación deberá ser realizada a una casilla de correo electrónico indicada por el titular al momento de realizar la reclamación.

Personales que no acoja a tramitación un reclamo, y la resolución que resuelve la reclamación, podrán siempre ser impugnadas judicialmente dentro del plazo de 15 días contados desde su notificación, a través del procedimiento establecido en el artículo 47 del Proyecto.

Queda claro, a partir de lo expuesto, que este procedimiento "no busca sancionar infracciones, sino que intenta proteger el derecho del titular en términos de hacer efectivo, por la vía administrativa o judicial, el ejercicio de los derechos que le reconoce la ley"[176]. Siendo destacable el esfuerzo del legislador por radicar en la Agencia este proceso de reclamación, debido a que como ha señalado parte de la doctrina el establecimiento de un procedimiento de reclamación llevado a cabo por organismos especializados resulta más eficiente (siempre que existan atribuciones suficientes). Por tanto, resulta conveniente radicar el control de la observancia de la ley en una agencia independiente que además contemple atribuciones fiscalizadoras y sancionatorias[177], puesto que solo de esa forma podremos brindar una protección efectiva a las personas afectadas en sus derechos, quienes podrán abandonar el uso de otros mecanismos menos idóneos para satisfacer sus necesidades.

IV.1.2.- Procedimiento administrativo por infracción de ley

El artículo 46 del Proyecto da inicio al segundo procedimiento contemplado, este procedimiento se diferencia del estudiado con anterioridad debido a que no surge de la falta de respuesta frente a los requerimientos de un titular de datos, sino que se encuentra contemplado para los casos en que los responsables de datos incumplan o vulneren los principios, derechos y obligaciones establecidas la ley.

Este procedimiento sancionatorio será instruido, de acuerdo con el literal a) del artículo 46, por la Agencia de Protección de Datos Personales, la cual podrá iniciar dicho procedimiento de oficio o a petición de parte, como resultado de un proceso de fiscalización o a consecuencia de una reclamación presentada por un titular de datos. El Proyecto menciona que, en este último caso, se deberá certificar la recepción del reclamo presentado por el titular[178].

Además, el procedimiento administrativo de infracción de ley, al igual que el procedimiento de reclamación, no podrá superar los seis meses; en caso de que se verifique que ha transcurrido más de seis meses desde la fecha de la certificación, indicada en la letra

[176] COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Op. Cit. p.423.
[177] LARA, J., VERA, F. y SOTO, B. Op. Cit. p. 32.
[178] Artículo 46 b)

b) del artículo 46, sin que la Agencia de Protección de Datos Personales haya resuelto la reclamación, el interesado podrá presentar un reclamo de ilegalidad en los términos previstos en el artículo 47 del Proyecto.

Ahora bien, una vez iniciado el procedimiento sancionatorio la Agencia deberá presentar una formulación de cargos en contra del responsable de datos[179] en la cual se deberán detallar los hechos que configuran la infracción, los principios y obligaciones incumplidos o vulnerados por el responsable, así como también la enunciación de las normas legales infringidas y cualquier otro antecedente que sirva para sustentar la formulación.

Por su parte, el responsable de datos tendrá un plazo de 15 días para presentar sus descargos acompañando todos los antecedentes que estime pertinente para desacreditar los hechos imputados por parte de la Agencia, para esto el responsable de datos podrá solicitar a la Agencia todas las medias o diligencias probatorias que estime necesarias[180]. Una vez recibidos los descargos o transcurrido el plazo otorgado para ello, la Agencia procederá a abrir un término probatorio de 10 días, siempre que se acredite la existencia de hechos sustanciales, pertinentes y controvertidos. Una cuestión relevante dentro de este procedimiento es que tanto los hechos investigados como las responsabilidades de los presuntos infractores podrán acreditarse mediante cualquier medio de prueba admisible en derecho, los que deberán ser apreciados de acuerdo con las reglas de la sana crítica.

Finalmente, La resolución que ponga fin al procedimiento sancionatorio deberá ser fundada y resolver todas las cuestiones planteadas en el expediente, debiendo pronunciarse sobre cada una de las alegaciones y defensas formuladas por el responsable de datos, además de contener la declaración de haberse configurado el incumplimiento o vulneración de los principios, derechos y obligaciones establecidos en la ley por el responsable o su absolución, según corresponda[181]. En caso de que la Agencia de Protección de Datos Personales considere que se ha verificado la infracción, en la misma resolución ponderará las

[179] Artículo 46: *"d) La formulación de cargos debe notificarse al responsable de datos a la dirección de correo electrónico señalada en la letra c) del artículo 14 ter.".*
[180] Artículo 46: *"g) La Agencia de Protección de Datos Personales dará lugar a las medidas o diligencias probatorias que solicite el responsable en sus descargos, siempre que sean pertinentes y necesarias. En caso de rechazo, deberá fundar su resolución.".*
[181] Artículo 46: *"i) La Agencia de Protección de Datos Personales tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución.".*

circunstancias que agravan o atenúan la responsabilidad del infractor e impondrá la sanción que corresponda de acuerdo con la gravedad de la infracción cometida[182].

En cuanto a las sanciones cabe destacar que el Proyecto contempla, en su artículo 39, un catálogo de sanciones en base a las diversas infracciones que el mismo cuerpo normativo contiene. Así, se establece que las infraccione leves[183] serán sancionadas con amonestación escrita o multa de 1 a 50 UTM; las infracciones graves[184] serán sancionadas con multa de 51

[182] Artículo 46: *"k) La resolución que establezca el incumplimiento o vulneración a los principios, derechos y obligaciones de esta ley y aplique la sanción correspondiente deberá ser fundada. Esta resolución debe indicar los recursos administrativos y judiciales que procedan contra ella en conformidad a esta ley, los órganos ante los que deben presentarse y los plazos para su interposición. La resolución de la Agencia de Protección de Datos Personales que resuelve el procedimiento por infracción de ley será reclamable judicialmente conforme al artículo siguiente.".*

[183] "Artículo 38 bis.- **Infracciones leves.** *Se consideran infracciones leves las siguientes:*
a) Incumplimiento total o parcial del deber de información y transparencia.
b) Carecer de un domicilio o de una dirección de correo electrónico o de un medio electrónico equivalente, actualizado y operativo, a través del cual los titulares de datos puedan dirigir sus comunicaciones o ejercer sus derechos.
c) Omitir la respuesta, responder en forma incompleta o fuera de plazo, las solicitudes formuladas por el titular de datos en conformidad a esta ley.
d) Omitir el envío a la Agencia de Protección de Datos Personales las comunicaciones previstas obligatoriamente en esta ley o sus reglamentos.
e) Incumplimiento de las instrucciones generales impartidas por la Agencia de Protección de Datos Personales en los casos que no esté sancionado como infracción grave o gravísima.
f) Cometer cualquier otra infracción a los derechos y obligaciones establecidas en esta ley, que no sea calificada como una infracción grave o gravísima.".

[184] *"Artículo 38 ter.-* ***Infracciones graves.*** *Se consideran infracciones graves las siguientes:*
a) Tratar los datos personales sin contar con el consentimiento del titular de datos o sin una base que otorgue licitud al tratamiento, o tratarlos con una finalidad distinta de aquélla para la cual fueron recolectados.
b) Comunicar o ceder datos personales del titular sin su consentimiento, siendo necesario contar con aquel o cederlos para un fin distinto del autorizado.
c) Efectuar tratamiento de datos personales innecesarios en relación con los fines del tratamiento.
d) Tratar datos personales inexactos, incompletos o desactualizados en relación con los fines del tratamiento.
e) Impedir u obstaculizar el ejercicio legítimo de los derechos de acceso, rectificación, cancelación, oposición o portabilidad del titular.
f) Omitir la respuesta, responder tardíamente o denegar la petición sin causa justificada, en los casos de solicitudes fundadas de bloqueo temporal del tratamiento de datos personales de un titular.
g) Realizar tratamiento de datos personales de niños, niñas y adolescentes con infracción a las normas previstas en esta ley.
h) Realizar tratamiento de datos personales sin cumplir los requisitos establecidos para las personas jurídicas de derecho privado sin fines de lucro y cuya finalidad sea política, filosófica, religiosa, cultural, sindical o gremial, respecto de los datos de sus asociados.
i) Vulnerar el deber de secreto o confidencialidad establecido en el artículo 14 bis.
j) Vulnerar o infringir las obligaciones de seguridad en el tratamiento de los datos personales establecidas en el artículo 14 quater.
k) Omitir las comunicaciones o los registros en los casos de vulneración de las medidas de seguridad establecidas en el artículo 14.
l) Adoptar medidas de calidad y seguridad insuficientes o no idóneas para el tratamiento de datos personales con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público.
m) Realizar operaciones de transferencia internacional de datos en contravención a las normas previstas en esta ley.
n) Incumplimiento de una resolución o un requerimiento específico y directo que le haya impartido la Agencia de Protección de Datos Personales.".

a 500 UTM; y las infracciones gravísimas[185] deberán ser sancionadas con multa de 501 a 5.000 UTM. Además, la Agencia podrá observar, en el establecimiento de las sanciones, las circunstancias atenuantes u agravantes de responsabilidad que se consideran en el Artículo 40 del Proyecto, así como también las reglas contenidas en el artículo 41.

IV.2.- PROCEDIMIENTO DE RECLAMACIÓN JUDICIAL

En primer lugar, es importante señalar que este procedimiento, contemplado en el artículo 47 del Proyecto, a diferencia de los anteriores no se debe llevar a cabo ante la Agencia de Protección de Datos Personales, sino que su competencia se encuentra radicada ante las diversas Cortes de Apelaciones de nuestro país.

En este procedimiento, las personas naturales o jurídicas, agraviadas[186] por una resolución final o de término de la Agencia podrán deducir un reclamo de ilegalidad ante la

---

[185] "Artículo 38 quater- **Infracciones gravísimas.** Se consideran infracciones gravísimas las siguientes:
a) Efectuar tratamiento de datos personales en forma fraudulenta.
b) Destinar maliciosamente los datos personales a una finalidad distinta de la consentida por el titular o prevista en la ley que autoriza su tratamiento.
c) Comunicar, transmitir o ceder, a sabiendas, información no veraz, incompleta, inexacta o desactualizada sobre el titular de datos.
d) Vulnerar el deber de secreto o confidencialidad sobre los datos personales sensibles y datos personales relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias.
e) Tratar, comunicar o ceder, a sabiendas, datos personales sensibles o datos personales de niños, niñas y adolescentes, en contravención a las normas de esta ley.
f) Omitir en forma deliberada la comunicación de las vulneraciones a las medidas de seguridad que puedan afectar la confidencialidad, disponibilidad o integridad de los datos personales.
g) Efectuar tratamiento masivo de datos personales contenidos en registros electrónicos de infracciones penales, civiles, administrativas y disciplinarias, que llevan los organismos públicos, sin contar con autorización legal para ello.
h) Realizar a sabiendas operaciones de transferencia internacional de datos en contravención a las normas previstas en esta ley.
i) Incumplimiento de una resolución de la Agencia de Protección de Datos Personales que resuelve la reclamación de un titular sobre el ejercicio de sus derechos de acceso, rectificación, cancelación, oposición, portabilidad o bloqueo temporal.
j) Entregar información falsa, incompleta o manifiestamente errónea en el proceso de registro o certificación del modelo de prevención de infracciones.".

[186] La redacción original del artículo 47 del Proyecto utilizaba la expresión "afectadas" y fue decisión de la Comisión el cambiarla por el término "agraviadas" en consideración a las recomendaciones realizadas por la Corte Suprema la cual señaló, en su Oficio N° 63-2017, del 3 de mayo de 2017, lo siguiente:
"Que si bien en términos generales la norma propuesta se encuentra acorde con la ponencia de la Corte, pueden formularse algunas observaciones en pro de la coherencia del sistema que se plantea. Como sucede, por ejemplo, con el concepto de "perjuicio" que utiliza la norma, que genera ambigüedades, en el sentido de producir cuestionamientos como: ¿se requerirá de un perjuicio económico, claramente identificable o bastará con acreditar un perjuicio de cualquier índole? ¿El concepto exigiría entonces, la acreditación de un perjuicio propiamente tal, o se refiere más a una especie de agravio? Esta última alternativa parece más acorde con las disposiciones procedimentales de la reclamación, que exigen identificar "las razones por las cuales el acto le perjudica".

Corte de Apelaciones de Santiago o a la que le corresponda según su domicilio (la cuestión queda entregada al arbitrio del reclamante) dentro del plazo de 15 días, contados desde el acto de notificación de la resolución impugnada.

El reclamante deberá individualizar en su escrito la resolución objeto del reclamo, además de señalar las normas legales que se estimen infringidas, la forma en que se ha producido la infracción, y cuando procediere, las razones por las cuales el acto le causa agravio. Lo anterior es importante ya que la Corte de Apelaciones respectiva podrá declarar inadmisible la reclamación si el escrito no cumple con las condiciones antes mencionadas según dispone el literal b) del artículo 47[187].

Una vez recibida la reclamación, la Corte de Apelaciones requerirá de informe a la Agencia, concediéndole para dichos efectos un plazo de diez días. Además, evacuado el traslado o teniéndosele por evacuado en rebeldía, la Corte de Apelaciones podrá, si es que estima necesario, abrir un término probatorio que se regirá por las reglas de los incidentes contempladas en el Código de Procedimiento Civil[188]. Vencido el término de prueba, se ordenará traer los autos en relación, gozando la vista de esta causa de preferencia para su inclusión en la tabla.

En tal sentido, cabe señalar que respecto a la información que el Estado puede restringir, la Corte Interamericana también se ha pronunciado, señalando una serie de estándares que pueden dar luces sobre el agravio exigible para dar paso a esta reclamación lo cual habrá de tenerse en cuenta al afinar la normativa de que se trata. Así lo ha manifestado en el caso Claude Reyes v. Chile.".
Sobre esta observación, el asesor del Ministerio de Hacienda, señor Godoy, hizo presente que la nueva redacción sugerida por el Ejecutivo es posterior al informe de la Excma. Corte Suprema, y las observaciones formuladas por el Máximo Tribunal fueron recogidas en esta nueva disposición.". En: COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Op. Cit. p. 535.

[187] Asimismo, podrá decretar orden de no innovar cuando la ejecución del acto impugnado le produzca un daño irreparable al recurrente.

[188] A este respecto es relevante destacar los artículos 89, 90 y 91 del Código de Procedimiento Civil, los cuales señalan:

"Art. 89. Si se promueve un incidente, se concederán tres días para responder y vencido este plazo, haya o no contestado la parte contraria, resolverá el tribunal la cuestión, si, a su juicio, no hay necesidad de prueba. No obstante, el tribunal podrá resolver de plano aquellas peticiones cuyo fallo se pueda fundar en hechos que consten del proceso, o sean de pública notoriedad, lo que el tribunal consignará en su resolución.

Art. 90. Si es necesaria la prueba, se abrirá un término de ocho días para que dentro de él se rinda y se justifiquen también las tachas de los testigos, si hay lugar a ellas.

Dentro de los dos primeros días deberá acompañar cada parte una nómina de los testigos de que piensa valerse, con expresión del nombre y apellido, domicilio y profesión u oficio. Sólo se examinarán testigos que figuren en dicha nómina.

Cuando hayan de practicarse diligencias probatorias fuera del lugar en que se sigue el juicio, podrá el tribunal, por motivos fundados, ampliar una sola vez el término por el número de días que estime necesarios, no excediendo en ningún caso del plazo total de treinta días, contados desde que se recibió el incidente a prueba.

Las resoluciones que se pronuncien en los casos de este artículo son inapelables.

Art. 91. Vencido el término de prueba, háyanla o no rendido las partes, y aún cuando éstas no lo pidan, fallará el tribunal inmediatamente o, a más tardar, dentro de tercero día, la cuestión que haya dado origen al incidente.".

Finalmente, si la Corte da lugar al reclamo, en su sentencia decidirá si existió agravio y ordenará, según sea procedente, la rectificación del acto impugnado y la dictación de la respectiva resolución, según corresponda[189]. Además, tratándose de reclamaciones en contra de una resolución que resuelve un procedimiento sancionatorio, la Corte podrá confirmar o revocar la resolución impugnada, establecer o desechar la comisión de la infracción, según corresponda y, mantener, dejar sin efecto o modificar la sanción impuesta al responsable o su absolución, según sea el caso[190].

CAPÍTULO V: ANÁLISIS COMPARADO, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD)

La creación de un órgano autónomo encargado de la protección de derechos de los titulares de datos no es una innovación de nuestro proyecto modificatorio analizado en los capítulos anteriores de este trabajo, sino que responde a la necesidad de acercar a nuestro país a los estándares internacionales exigidos, permitiendo que nuestro sistema se equipare respecto de aquellos Estados que ya consagran, dentro de su sistema jurídico, una autoridad de control independiente y especializada.

En el continente europeo la protección de datos personales es un tema que ha tomado relevancia desde hace largo tiempo, ejemplo de esto es el hecho de se aprobara, en 1981, "el Convenio n.º 108 del Consejo, sobre la protección de las personas en lo relativo al tratamiento automatizado de datos de carácter personal, primera norma europea que marcó las pautas del modelo común de protección de datos. El Convenio pretendía ampliar la protección de los derechos y las libertades fundamentales y, en concreto, el derecho al respeto a la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos informatizados."[191]

En la actualidad, la "piedra angular de esta serie de medidas de protección, ha sido el Reglamento (UE) 2016/67934 General de Protección de Datos. El Reglamento tiene por objeto garantizar la protección de datos de las personas físicas en toda la Unión Europea de forma

[189] Artículo 47 f).
[190] Artículo 47 h).
[191] BRU CUADRADA, E. La protección de datos en España y en la unión europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad. *Revista de Internet, Derecho y Política,* Universitat Oberta de Catalunya, Número 5, 2007, pp. 78-92. p. 82. [En línea]: https://dialnet.unirioja.es/descarga/articulo/2372618.pdf [Consulta: 29 de Noviembre 2021]

uniforme y ofreciendo siempre los más altos niveles de protección, entró en vigor el 24 de mayo de 2016, es de aplicación desde el 25 de mayo de 2018 y nació con la finalidad de establecer una única norma en la Unión Europea con el propósito de acabar con la fragmentación legislativa existente hasta entonces, así como las costosas cargas administrativas que se derivaban de los diferentes tratamientos de datos. El Reglamento busca beneficiar tanto a los ciudadanos a la hora de ejercer sus derechos como a las empresas al simplificar las normas que se les aplican, para la Unión Europea ha sido una medida esencial para fortalecer los derechos fundamentales de los ciudadanos en la era digital y que, en definitiva, persigue alcanzar la unificación del derecho comunitario de acuerdo con las exigencias de la sociedad tecnológica actual."[192]

Así, al alero de dicho Convenio, y de otras normativas comunitarias sobre datos personales, los Estados europeos fueron adoptando normativas particulares que pretendieron regular el tratamiento de datos personales, estableciendo para tales efectos autoridades de control independientes[193]. Tal es el caso de España, la cual consagra dentro de su sistema a la Agencia Española de Protección de Datos (en adelante también "AEPD") como la entidad garante de la protección de los derechos de los titulares de datos[194]. El análisis de las características más relevantes de la AEPD resulta importante en el estudio de nuestra pretendida Agencia, ya que gran parte de las críticas a nuestra actual legislación se hacen en consideración a las características de la AEDP, así, por ejemplo, se ha señalado que mientras "que España establece potestades oficiosas de control, instrucción y sanción para la AEPD, sin perjuicio de que el individuo pueda accionar en sede jurisdiccional para obtener resarcimiento patrimonial, Chile descansa esencialmente sobre el impulso de los particulares para poner en marcha los mecanismos institucionales (administrativos y judiciales) de

[192] TALENS, Á. La protección de datos personales como un derecho fundamental en la era de la tecnología y su protección en el ordenamiento jurídico español. Universidad de Jaén, 2019. p. 19. [En línea]: http://tauja.ujaen.es/bitstream/10953.1/10829/1/TFG_Alvaro_Talens_2805_.pdf [consulta: 24 de Noviembre 2021].

[193] Así, por ejemplo, se puede mencionar los siguientes Estados europeos que consagran autoridades de control independientes del Poder Ejecutivo: *Komisioner per te drejtat e inform mit dhe brojtjen e te dhenave persona (Information and Data Protection Commisioner)* **(Albania)**; *Federal Commissioner for Data protection and freedom of Information* **(Alemania)**; *Information Commissioner of Slovenia.* **(Eslovenia)**; *Hungarian National Authority for Data Protection and Freedom of Information* **(Hungría)**; *Information Commissioner's Office (ICO)* **(Inglaterra)**; *Office of the Information and Data Protection Commissioner* **(Malta);** *The Commissioner for Information of Public Importance and Personal Data Protection* **(Serbia);** *Federal Data Protection and Information Commissioner.* **(Suiza).** En; CONSEJO PARA LA TRANSPARENCIA. Experiencia comparada sobre la consagración constitucional del derecho de acceso a la información y la protección de datos personales. *Op. Cit.* pp. 29-30.

[194] Cabe destacar que "España es una nación descentralizada, compuesta por diecisiete comunidades autónomas en la que están delegadas sus competencias; por eso, cada comunidad autónoma tiene su autoridad de protección de datos, las cuales también son independiente en su ejercicio". En: MORALES, S. La Agencia Española de Protección de Datos: Un estudio breve sobre su naturaleza jurídica, su régimen jurídico y su estructura tanto estatal como autonómica. *NovumJus*, V. 14, Núm.2, 2020, pp. 173-194. p. 192. [En Línea]:https://novumjus.ucatolica.edu.co/article/view/3078 [Consulta: 22 Noviembre 2021].

protección de datos personales, y descansa sobre la decisión, capacidad técnica y económica de dichos particulares para sustanciar procedimientos, ya sea contra la Administración del Estado o contra empresas o individuos especializados en tecnologías de la información. La asimetría entre particulares, por un lado, y Estado y empresas de tecnología, por otro, pone en entredicho la efectividad de los mecanismos de protección de datos personales propuestos en la reforma."[195]

Adicionalmente, como se ha mencionado con anterioridad en este trabajo, la legislación española ha sido el marco referencial a partir del cual se ha estructurado el sistema de protección de datos personales en nuestro país y, por tanto, resulta fundamental comprender qué características ha adoptado nuestra nueva legislación en materia de protección de datos personales que puedan presentar un vínculo con la actual normativa en materia de protección de datos en el país europeo.

V.1.- CREACIÓN

En España, la "creación de la Agencia Española de Protección de Datos (AEPD) se produjo mediante la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, la cual contenía su diseño institucional básico, sus funciones, órganos y el régimen jurídico; fue un avance jurídico en el ámbito del Legislador español y además establecía los límites en el uso de la informática, así como la protección de datos.

La Ley Orgánica 5/1992 desarrollaba el Artículo 18.4 de la Constitución española, el cual se incardina en un precepto dedicado a la protección de la intimidad de los ciudadanos. Posteriormente, desde el ámbito de la Unión Europea, la Directiva 95/46/ CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, llegó a rellenar el vacío existente en la legislación comunitaria respecto a la protección de los datos personales. Ya en el siglo XXI, el Legislador español emitió la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales (LOPD) y se unió con el Legislador europeo mediante el Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (RGPD). Por otra parte, el Legislador español conservó los Estatutos

[195] BECERRA, P. Potestades sancionatorias en el proyecto de reforma a la Ley N° 19.628 de Protección de Datos personales. Una crítica. *Revista de Derecho,* Escuela de Postgrado N°3, 2013, pp. 163-192. p.186.

de la AEPD, mediante el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos."[196]

Así, según versa el artículo 41 de la Ley Orgánica 3/2018, la AEPD se erige como una autoridad administrativa independiente, de carácter público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones[197]. "La Agencia Española de Protección de Datos propende por el cumplimiento de la ley de protección de datos de carácter personal, así como de los derechos a información, acceso, oposición y supresión de datos de carácter personal, tanto para las personas jurídicas como para las personas físicas. Su función es atender peticiones o reclamaciones y prestar la información que necesiten, pues esta es un derecho fundamental. Además, le corresponde elaborar informes dentro del ámbito de su normativa, así como disposiciones relativas a su potestad y la adopción de normas reglamentarias."[198]

V.1.1.- Independencia

En la doctrina española se ha destacado que el requisito de independencia de las autoridades de protección de datos frente a la actuación de otros poderes públicos es una de las condiciones *sine qua non* para que sea posible considerar que las legislaciones nacionales reguladoras de las mismas cumplen plenamente con los requisitos de transposición de la normativa comunitaria (de la Unión Europea) en esta materia[199]. En dicho sentido, se ha señalado que el legislador "pensó dar un mayor uso a la Agencia Española de Protección de Datos (AEPD), primeramente, por ser independiente de la autoridad administrativa estatal y por tener capacidad jurídica pública y privada"[200], siendo importante recalcar que el actuar independiente de la AEPD "redundará en el buen desempeño de sus funciones de control llevados a cabo tanto por el sector público como por el privado."[201]

---

[196] MORALES, S. Op. Cit. p. 176.
[197] Esta consagración de una entidad especializada e independiente dice relación con lo establecido en el artículo 51 del Reglamento general de Protección de Datos (RGPD) el cual establece que "Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante «autoridad de control») supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión."
[198] MORALES, S. Op. Cit. 191
[199] PUENTE, A. La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal. En: *Azpilcueta: cuadernos de derecho*, Núm. 20, 2008, pp.13-41, p. 26 [En Línea]: https://core.ac.uk/download/pdf/11501783.pdf [Consulta: 26 de Noviembre 2021]
[200] MORALES, S. Op. Cit. p. 178.
[201] PUENTE, A. Op. Cit. p. 27.

En torno a esto podemos señalar que nuestro Proyecto resulta asertivo, toda vez que establece la autonomía de nuestra pretendida Agencia, cuestión que implica un primer punto de similitud entre nuestra autoridad y la AEPD. Como ya se destacó anteriormente, este carácter autónomo permite establecer un alto estándar de eficacia y diligencia en la protección de los principios y derechos que regulan esta materia, finalidad que no se obtiene al radicar competencias en órganos cuya funcionalidad responde a otras materias o principios como es el caso del CPTL o el SERNAC dentro del ordenamiento chileno, todo esto en base a los comentarios realizados en los apartados respectivos del presente trabajo.

La idea de independencia de la autoridad de control en el proyecto modificatorio de la Ley N° 19.628, que se observa también en la AEPD, permite elevar nuestro sistema de protección de datos a los estándares europeos vigentes, los cuales exigen una entidad dotada de la debida independencia de la administración estatal; por otra parte, también nos permitirá ser considerados como un país seguro en torno al tratamiento de datos personales, esto debido a que contaremos con una institucionalidad fuerte en la protección de los derechos de los titulares y que no se encontrará sujeta a injerencias externas que puedan desvirtuar la funcionalidad de la autoridad de control.

V.2.- ORGÁNICA

V.2.1.- Presidencia

La Presidencia de la AEPD[202], según establece la Ley Orgánica 3/2018, será nombrada por el Gobierno, a propuesta del Ministerio de Justicia, dentro de un grupo de candidatos considerados en base a su reconocida competencia profesional en materia de protección de datos[203]. En torno a este punto es importante destacar que nuestro Proyecto hace eco de la necesidad de que quien ostente el cargo de Director de la autoridad de control cuente con los conocimientos necesarios en materia de protección de datos, esta cuestión no solo es relevante en cuanto al buen desempeño del cargo, sino que también respecto de la visión de políticas públicas que permitan ir desarrollando mejoras en la materia teniendo en consideración las innovaciones internacionales.

[202] Así como también la figura del “Adjunto”, quien es considerado como un auxiliar de la persona que ostente la Presidencia de la AEPD.
[203] Art. 48 Ley Orgánica 3/2018.

Un punto dirimente entre la Presidencia de la AEPD y nuestra Agencia es la participación en la designación del Director de diversos poderes del Estado. En nuestro Proyecto se considera la participación del Senado, en cambio, en la AEPD sólo se observa la participación del Poder Ejecutivo en la designación. Así, en favor de la independencia debida que debe revestir el cargo de Director y la Agencia misma, es preferible el sistema de nombramiento que contempla nuestro Proyecto en base a dos razones, "la primera, el incipiente y/o precario desarrollo del asociacionismo necesario para entregar el nombramiento de alguno de los miembros de la autoridad de control a cuerpos intermedios; y, la segunda, la atribución de un cometido esencialmente técnica que demanda conocimientos altamente especializados entre quienes cumplen labores en la autoridad de control."[204]

Por otra parte, se establece que la duración del cargo de Presidente de la AEPD se contendrá en un periodo de 5 años, pudiendo renovarse en el cargo por el mismo período de tiempo[205]. Esto refleja una similitud respecto de nuestro Proyecto, el cual contempla un mismo período de tiempo para el ejercicio del cargo de Director, así como también la posibilidad de renovación por un mismo lapso de tiempo. Esta cuestión, como ya se analizó con anterioridad, es indispensable dentro de una autoridad de control, ya que permite que el más alto cargo dentro del órgano no se vea afecto a los cambios del ciclo político dentro del propio Estado, evitando que su designación del Director de la autoridad de control se vea influida por el ascenso de diversas corrientes políticas en el gobierno.

Finalmente, la normativa nos señala que quien ostente la Presidencia de la AEPD cesará en su cargo (antes de la expiración del período correspondiente) a petición propia o por acuerdo del Consejo de Ministros sobre cuatro causales especificas: a) Incumplimiento grave de sus obligaciones; b) incapacidad sobrevenida para el ejercicio de su función; c) incompatibilidad; d) condena firme por delito doloso[206]. En torno a esto "no cabe duda que tratándose de una autoridad a la cual desea conferírsele cierta autonomía para el desempeño de su cometido, debe adjudicársele ciertas garantías de que las decisiones que haya de adoptar no condicionarán su permanencia en el cargo[207]", siendo importante el establecimiento de causales específicas que digan relación con otros aspectos relevantes como los antes señalados. Cabe destacar que nuestro Proyecto también contempla un catálogo de inhabilidades y causales de destitución del cargo, cumpliéndose con esto el respeto a la

[204] CERDA, A. Op. Cit. p. 194.
[205] Art. 48 N°5 Ley Orgánica 3/2018.
[206] Idem.
[207] CERDA, A. Op. Cit. p. 195.

independencia de la autoridad de control ya que ninguna de las causales dicen relación con las decisiones que tome el Director en el desempeño de su cargo.

V.2.2.- Consejo Consultivo

Ahora bien, a pesar de las similitudes señaladas con anterioridad, una diferencia orgánica importante respecto de la Agencia que se pretende instaurar en nuestro país viene dada por el hecho de que en la estructura de la AEPD se comprende un "Consejo Consultivo"[208], el cual es concebido como el encargado de asesorar a la Presidencia de la AEPD[209]; aunque es importante señalar que esta facultad se ve disminuida al observar que, por disposición expresa, sus decisiones no tendrán en ningún caso carácter vinculante para el Presidente o Director de la AEPD. Así, este Consejo "goza de facultades bastante mitigadas, cuyo cometido se reduce a asistir al Director y ser oídos en el expediente de destitución del mismo, en tanto que sus informes no son vinculantes"[210].

En el proyecto modificatorio que consagra nuestra Agencia no se otorga un apartado a la creación de una entidad similar, dejando al Director de la Agencia como el único responsable a cargo de las directrices de la Agencia[211]. En torno a esto es del todo pertinente señalar que la confección de un Consejo puede resultar beneficioso para el funcionamiento de la Agencia, ya que como se observa en el caso de la AEPD el Consejo se encuentra conformado por especialistas en materia de protección de datos que pueden, desde sus esferas de

---

[208] El Consejo Consultivo se encuentra conformado por: *a) Un Diputado, propuesto por el Congreso de los Diputados; b) Un Senador, propuesto por el Senado; c) Un representante designado por el Consejo General del Poder Judicial; d) Un representante de la Administración General del Estado con experiencia en la materia, propuesto por el Ministro de Justicia; e) Un representante de cada Comunidad Autónoma que haya creado una Autoridad de protección de datos en su ámbito territorial, propuesto de acuerdo con lo que establezca la respectiva Comunidad Autónoma; f) Un experto propuesto por la Federación Española de Municipios y Provincias; g) Un experto propuesto por el Consejo de Consumidores y Usuarios; h) Dos expertos propuestos por las Organizaciones Empresariales; i) Un representante de los profesionales de la protección de datos y de la privacidad, propuesto por la asociación de ámbito estatal con mayor número de asociados.; j) Un representante de los organismos o entidades de supervisión y resolución extrajudicial de conflictos previstos en el Capítulo IV del Título V, propuesto por el Ministro de Justicia; k) Un experto, propuesto por la Conferencia de Rectores de las Universidades Españolas; l) Un representante de las organizaciones que agrupan a los Consejos Generales, Superiores y Colegios Profesionales de ámbito estatal de las diferentes profesiones*
colegiadas, propuesto por el Ministro de Justicia; m) Un representante de los profesionales de la seguridad de la información, propuesto por la asociación de ámbito estatal con mayor número de asociados; n) Un experto en transparencia y acceso a la información pública propuesto por el Consejo de Transparencia y Buen Gobierno; ñ) Dos expertos propuestos por las organizaciones sindicales más representativas

[209] Art. 49 Ley Orgánica 3/2018.

[210] CERDA, A. La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales. Op. Cit. p. 185.

[211] Actuar que, como se señaló en este trabajo al revisar las facultades de la Agencia, deberá observar un deber de coordinación con el Consejo para la Transparencia.

conocimiento, aportar y ayudar a generar mecanismos de control preventivos eficaces, entregar directrices que permitan establecer sistemas y obligaciones de tratamiento de datos más seguros, así como también generar normas que permitan dar una adecuada protección a las diversas categorías de datos personales dentro de nuestro ordenamiento jurídico.

V.3.- FUNCIONES Y POTESTADES

El artículo 47 de la Ley Orgánica 3/2018 establece, en su artículo 47, que será función de la AEPD supervisar la aplicación de las disposiciones contenidas en el mismo cuerpo normativo y, además, velar por la aplicación del Reglamento (UE) 2016/679, con especial énfasis en el ejercicio de las funciones establecidas en los artículos 57 y 58 de dicho Reglamento.

Así, de la lectura de los artículos 57 y 58 del reglamento (UE) 2016/679 se puede señalar como principales funciones, en atención a la comparativa pretendida, las siguientes:

- *Promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento*[212]. Esta facultad se puede evidenciar en nuestra Agencia, ya que se consagra en el Proyecto como una de las facultades de la autoridad el "desarrollar programas, proyectos y acciones de difusión, educación, promoción e información dirigidos a la ciudadanía y a los responsables de datos"[213]. Se debe apreciar positivamente el hecho de haber otorgado esta facultad a nuestra Agencia, ya que representa el ejercicio activo, por parte de un órgano del Estado, en la difusión de los derechos que poseen los titulares sobre sus datos, permitiendo con esto que la ciudadanía tenga un mayor conocimiento y comprensión de los derechos que poseen en materia de datos personales, independientemente de si estos dicen relación con aspectos sensibles de su persona.
- *Asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento*[214]*.* Esta función también la vemos presente en nuestra Agencia, ya que ésta podrá proponer al presidente de la República las normas

[212] Artículo 57 b) Reglamento (UE) 2016/679.
[213] Artículo 31 h) modificado por la Comisión.
[214] Artículo 57 c) Reglamento (UE) 2016/679.

legales y reglamentarias que permitan dar una mayor protección de los datos personales de las personas. Esta función resulta importante en cuanto nuestra Agencia, al igual que la AEPD, son órganos técnicos y profundamente especializados en la materia, cuestión por la cual las recomendaciones que emanen por parte de dichos órganos es de vital importancia en la elaboración de normativas que tiendan a la protección de los derechos de los titulares de datos.

- *Tratar las reclamaciones presentadas por un interesado o por un organismo e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable*[215]*.* Esto se relaciona directamente con la facultad de nuestra Agencia de poder conocer y resolver las reclamaciones que formulen los titulares de datos por las afectaciones que puedan sufrir. Reviste toda lógica que nuestra autoridad de control cuente con esta facultad, ya que es la expresión básica de la funcionalidad de la Agencia en el ámbito de la protección de datos personales.
- *La autoridad de control podrá establecer una tasa razonable basada en los costes administrativos o negarse a actuar respecto solicitudes que sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo.* Esta facultad no aparece contemplada dentro del Proyecto, pero se advierte que una estipulación en tal sentido puede ser beneficiosa en términos de volumen de trabajo de la Agencia, toda vez que el establecimiento de tasas, ante solicitudes repetitivas, es una forma de desincentivar la litigación excesiva frente a la Agencia; de no considerarse el establecimiento de dichas tasas se puede ver afecto el debido y correcto desempeño de sus funciones, y generar excesivas demoras en la tramitación de reclamaciones, las cuales (debido a su naturaleza) deben recibir un tratamiento expedito y eficaz.
- *Sancionar a todo responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el Reglamento; Sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el Reglamento*[216]*.* Nuestra Agencia cuenta, dentro del Proyecto, con poderes similares, en cuanto se permite investigar y determinar infracciones en que incurran responsables de datos. Esto es importante si lo que queremos es dotar a nuestra Agencia de un rol activo en la protección de los derechos de los titulares de datos.

[215] Artículo 57 f) Reglamento (UE) 2016/679.
[216] Artículo 58 N° 2, literales a) y b) Reglamento (UE) 2016/679.

- *Imponer una multa administrativa.* Es importante que las autoridades de control puedan imponer multas ante las infracciones que conozca en el ejercicio de sus funciones, toda vez que con esto se evita que se repliquen las conductas por parte de otros agentes que realicen tratamiento de datos. Nuestro Proyecto contempla la posibilidad de que la Agencia imponga multas a quienes infringen la normativa de la Ley y, en tal sentido, permite dotar a nuestra autoridad de control de un poder efectivo en la protección de los derechos de los titulares de datos.

V.4.- PROCEDIMIENTOS REGULADOS ANTE LA AEPD

Otra similitud destacable entre estas instituciones viene dada por la instauración de un procedimiento encaminado al conocimiento de las vulneraciones de derechos sobre datos personales (tutela de derechos)[217] y un régimen sancionador[218] de carácter administrativo mediante los cuales ambas agencias pueden conocer de las reclamaciones de particulares afectados en sus derechos e imponer un régimen de multas, en base a un catálogo graduado de sanciones cometidas, a un responsable de datos que infrinja la normativa correspondiente.

La Ley Orgánica 3/2018 establece, en su artículo 65, que cuando se presente ante la AEPD una reclamación, ésta deberá evaluar su admisibilidad a trámite, de conformidad con diversos supuestos como, por ejemplo, el hecho de que las reclamaciones presentadas no digan relación con cuestiones de protección de datos personales, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción.

Igualmente, la AEPD podrá inadmitir la reclamación cuando el responsable o encargado del tratamiento, previa advertencia formulada por la AEPD hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos[219]. En cuanto a esto, se evidencia en nuestro Proyecto la facultad de la Agencia de poder revisar la admisibilidad de las reclamaciones que titulares de datos le presenten, cuestión para la cual se establece un plazo de 10 días. Es importante remarcar nuestro Proyecto plantea un plazo considerablemente menor para el juicio de admisibilidad, cuestión que en la práctica permitirá generar un procedimiento que de protección al titular de forma mucho más efectiva y rápida; por contrapartida, el control de admisibilidad en el

[217] Regulado a partir del artículo 63 de la Ley Orgánica 3/2018.
[218] Art. 70 y ss. de la Ley Orgánica 3/2018.
[219] La decisión sobre la admisión o inadmisión a trámite deberá notificarse al reclamante en el plazo de tres meses.

procedimiento español resulta excesivo y puede producir, en ciertos casos, indefensión a los titulares producto de la demora en el conocimiento de los conflictos.

Además, establece la Ley española que, una vez admitida la reclamación, la AEPD podrá dictar acuerdo de inicio de procedimiento para el ejercicio de la potestad sancionadora, en que se concretarán los hechos, la identificación de la persona o entidad contra quien se reclama, la infracción que pudo haber cometido el encargado de datos y su posible sanción[220]. Una vez iniciado el procedimiento la AEPD podrá acordar, motivadamente, las medidas provisionales necesarias tendientes a salvaguardar el derecho fundamental a la protección de datos[221].

Al finalizar este procedimiento de infracción la AEPD podrá adoptar, de acuerdo a la gravedad de las infracciones establecidas, las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del reglamento (UE) 2016/796[222].

Este procedimiento de reclamación y la posterior aplicación de sanciones es un símil de lo que establece el Proyecto respecto de nuestra Agencia, ya que a esta última se le entrega la facultad de conocer de las reclamaciones a través de un procedimiento administrativo, para posteriormente establecerse en favor de ésta la facultad de establecer sancione y multas en base a un catálogo de infracciones debidamente graduadas en atención al nivel de afectación que puedan reportar a los titulares de datos.

La diferencia que se puede observar entre estos procedimientos dice relación con la prescripción de las acciones para perseguir la responsabilidad ante la comisión de alguna de las infracciones contenidas en las normativas respectivas. En primer lugar, en la legislación española se establece un régimen diferenciado de prescripción en base a la gravedad de la infracción[223], mientras que en nuestro Proyecto se contempla un único plazo de prescripción

[220] Artículo 68 Ley Orgánica 3/2018.
[221] Según versa el artículo 69 de la Ley Orgánica 3/2018: "2. En los casos en que la Agencia Española de Protección de Datos considere que la continuación del tratamiento de los datos personales, su comunicación o transferencia internacional comportara un menoscabo grave del derecho a la protección de datos personales, podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización.".
[222] Las multas tendrán un margen que irá desde los 10.000.000 EUR a 20.000.000 EUR, o tratándose de una empresa, las multas irán desde el 2% al 4% de del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.
[223] Respecto de las infracciones leves se establece un plazo de prescripción de un año; en cuanto a las infracciones graves se establece un plazo de prescripción de 2 años; finalmente, las infracciones consideradas muy graves tendrán un plazo de prescripción de 3 años.

de 3 años para perseguir la responsabilidad por las infracciones previstas en la ley, contados desde la ocurrencia del hecho que dio origen a la infracción[224].

En torno a esto, la posición de este autor es estimar correcta la decisión del legislador nacional de establecer un plazo único de prescripción para las acciones sobre infracciones a la normativa de protección de datos debido a que se está afectando un derecho fundamental contenido en nuestra Constitución y, por tanto, no parece ser conveniente que se consideren plazos diferenciados de prescripción en base a la magnitud de la afectación.

CAPÍTULO VI: SINTESIS Y CONCLUSIONES

De lo analizado en los capítulos precedentes es posible extraer la relevancia de la instauración de un organismo especializado y autónomo que vele por la protección de los derechos sobre datos personales dentro de nuestro país, en especial si tenemos en consideración que nos encontramos dentro una sociedad cada vez más tecnológica.

La creación de la Agencia de Protección de Datos Personales aparece como la solución correcta en un mundo en el que cada vez las interacciones son más numerosas y el flujo de datos personales es constante. El Estado debe abocarse de forma seria a la labor de proteger los datos de las personas y los derechos que se conceden a los titulares cuando estos se vean afectados por las prácticas que los organismos públicos o el mundo privado puedan realizar, especialmente respecto de estos últimos, ya que han hecho de los datos personales un bien altamente preciado en el comercio digital. El establecimiento de un organismo autónomo como la Agencia, con las facultades contenidas en el Proyecto (fiscalización, sanción y promoción de medidas que apunten a la protección de los datos personales), si bien implica un gasto fiscal mayor al que se puede generar si radicamos dichas facultades en órganos públicos ya existentes, nos permitirá acercarnos a los estándares internacionales y, por sobre todo, nos asegurará una debida protección ante prácticas de tratamiento indebido de datos en una sociedad donde la captura de datos, y su posterior tratamiento, son cada vez mayores. Debemos hacer frente, mediante una autoridad fuerte, a una sociedad en la cual los datos son transados con alto valor comercial, para así asegurar una protección efectiva.

[224] En la discusión dentro de la Comisión se dio cuenta, durante el examen del artículo 44 del Proyecto, que la moción con la que se refunde el informe disponía la diferenciación de plazos de prescripción de igual forma a como se establece en la legislación española. En: COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Op. Cit. p. 516.

Además, es importante que la autoridad de control posea las facultades fiscalizadoras y sancionadoras que contiene el Proyecto analizado para poder hacer frente de forma efectiva y eficaz a las conductas que puedan resultar vulneratorias de los derechos contenidos en la Ley. La creación de la Agencia de Protección de Datos consagrada en el proyecto estudiado es, a juicio de este autor, el camino correcto para alcanzar los fines de una protección efectiva de los principios y derechos emanados de nuestra normativa en materia de datos personales, cuestión que no se logrará si entregamos dichas facultades a organismos dependientes del poder ejecutivo u organismos abocados a materias que puedan tener ciertos puntos de conexión con la materia, pero que no son de su especialidad; sobre todo si tenemos en consideración que lo que se pretende proteger a través de una autoridad de control no es un simple derecho pecuniario, sino que es un derecho fundamental, cuestión que merece la más alta protección y la debida especialización por parte del órgano garante.

Una institucionalidad como la que representa la Agencia nos permitirá acercarnos a los estándares internacionales y confirmar a nuestro país como un Estado democrático que contiene mecanismos efectivos en la protección de los derechos, no solo como un ente castigador de las vulneraciones a dichos derechos, sino que también como un Estado activo en la promoción de los derechos de los titulares sobre datos personales.

Con lo expuesto se puede señalar que la Agencia (como organismo especializado) tendrá facultades que le permitirán establecer, respecto de aquellos que realicen tratamiento de datos (personalmente o a través de terceros) o aquellos que comercialicen paquetes de datos, una serie de deberes que, en la práctica, deberán ejecutarse de manera previa y permanente para garantizar el respeto del objeto de la protección de datos: el control de la información personal. Con esto se conformará, en la práctica, un verdadero requisito insoslayable que apunte a que la información deba ser tratada adoptando todas las medidas de carácter técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal, evitando su alteración, pérdida, tratamiento o acceso no autorizado[225].

En este sentido es importante tomar referencia de otras instituciones autónomas que han sido eficaces en diversos ordenamientos jurídicos como es el caso de la AEPD, agencia que responde a los más altos estándares internacionales y que puede ser tomado como un ejemplo adecuado, teniendo siempre en consideración las críticas (positivas y negativas) que

[225] GARRIDO, R. La seguridad en el tratamiento de datos personales. *Ciudadanas 2020 III, El Gobierno de la Información, Instituto Chileno de Derecho y Tecnologías,* 2015, pp. 77- 92, p. 81 [En línea]: https://www.icdt.cl/ciudadanas-2020-iii/ [Consulta: 30 Junio 2021]

la doctrina ha realizado, debido a la cercanía cultural que compartimos con España y teniendo en cuenta que la normativa española en materia de protección de datos ya fue considerada como un punto de referencia al momento de dictación de la Ley N° 19.628.

BIBLIOGRAFIA

- ÁLVAREZ, D. Acceso a la información pública y protección de datos personales: ¿puede el consejo para la transparencia ser la autoridad de control en materia de protección de datos?. *Revista de derecho (Coquimbo)*, *23*(1), 2016, pp. 51-79. [En Línea]: https://dx.doi.org/10.4067/S0718-97532016000100003
- ÁLVAREZ, D. La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa. *Revista Chilena de Derecho y Tecnología,* VOL. 9 N°1, 2020, pp. 1-4.
- AMCHAM CHILE. Comentarios de AmCham Chile a artículo 15 bis del Boletín 12.409-03.
- ARRIETA, R. Chile y la protección de datos personales: Compromisos internacionales. *VV.AA, Chile y la protección de datos personales: ¿están en crisis nuestros derechos fundamentales?,* Ediciones Diego Portales, 2009.
- BECERRA, P. Potestades sancionatorias en el proyecto de reforma a la Ley N° 19.628 de Protección de Datos personales. Una crítica. *Revista de Derecho,* Escuela de Postgrado N°3, 2013, pp. 163-192.
- BRU CUADRADA, E. La protección de datos en España y en la unión europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad. *Revista de Internet, Derecho y Política,* Universitat Oberta de Catalunya, Número 5, 2007, pp. 78-92. [En línea]: https://dialnet.unirioja.es/descarga/articulo/2372618.pdf
- CERDA, A. Autodeterminación Informativa y Leyes Sobre Protección de Datos. *Revista Chilena de Derecho Informático,* Núm. 3, 2003. pp. 47- 75.
- CERDA, A. La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales. Universidad de Chile, Facultad de Derecho, 2003. [En Línea]: http://repositorio.uchile.cl/handle/2250/106762
- COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Informe 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 Nos. 11.092-07 y 11.144 - 07, refundidos. [En Línea]: https://www.camara.cl/legislacion/ProyectosDeLey/informes.aspx?prmID=11661&prmBOLETIN=11144-07

- COMUNICACIÓN CONJUNTA DE DERECHOS DIGITALES, CIUDADANO INTELIGENTE, FUNDACIÓN PRO ACCESO, Y PRIVACY INTERNATIONAL. El derecho a la privacidad, 2019. [En Línea]: https://www.derechosdigitales.org/wp-content/uploads/EPU-Chile_Privacidad_Presentado-1.pdf
- CONSEJO PARA LA TRANSPARENCIA. Experiencia comparada sobre la consagración constitucional del derecho de acceso a la información y la protección de datos personales. Cuaderno de trabajo N°18, Dirección de Estudios, 2020.
- CONSEJO PARA LA TRANSPARENCIA. Fundamentos para definir al Consejo para la Transparencia como la autoridad de control en materia de protección de datos personales, 2019. [En Línea]: https://www.consejotransparencia.cl/wp-content/uploads/estudios/2020/01/Fundamentos-para-definir-al-Consejo-como-la-autoridad-PDP.pdf [Consulta: 27 Octubre 2021].
- CONSEJO PARA LA TRANSPARENCIA. Protección de Datos Personales en la era de la economía digital. *Cuaderno de trabajo N°15,* , 2020, [En Línea]: https://www.consejotransparencia.cl/wp-content/uploads/estudios/2020/10/Economi%CC%81a-digital-V4.pdf
- CONTRERAS, P. El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la constitución chilena. *Estudios Constitucionales,* vol. 18, núm. 2, 2020. pp. 87-120.
- CONTRERAS, P., TRIGO, P. Interés legítimo y tratamiento de datos personales: antecedentes comparados y regulación en Chile. *Revista de Derecho y Tecnología,* VOL. 8, Núm.1, 2019, pp. 69-196.
- CUMPLIDO, F. Análisis del anteproyecto de ley sobre protección de datos personales elaborado por el Ministerio de justicia (1990-1994).
- DEL VILLAR, L. El SERNAC y protección de datos, 2021. [En Línea]: https://www.sernac.cl/portal/604/w3-article-62885.html

- El debate sobre datos personales vuelve cardado de dudas sobre su financiamiento. En Pauta en internet. 30 de Junio, 2021. https://www.pauta.cl/economia/proyecto-datos-personales-costos-fiscales-consejo-para-transparencia
- GARRIDO, R. La seguridad en el tratamiento de datos personales. *Ciudadanas 2020 III, El Gobierno de la Información, Instituto Chileno de Derecho y Tecnologías,* 2015, pp. 77- 92. [En línea]: https://www.icdt.cl/ciudadanas-2020-iii/
- HERRERA, P. El derecho a la vida privada y las redes sociales en Chile. *Revista Chilena de Derecho y Tecnología,* Vol. 5, N°1, 2016, pp. 87-112.
- INFORME DE LA COMISIÓN DE ECONOMÍA, FOMENTO, MICRO, PEQUEÑA Y MEDIANA EMPRESA, PROTECCIÓN DE LOS CONSUMIDORES Y TURISMO RECAÍDO EN EL PROYECTO DE LEY QUE ESTABLECE MEDIDAS PARA INCENTIVAR LA PROTECCIÓN DE LOS DERECHOS DE LOS CONSUMIDORES. [En Línea]: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12940&prmBoletin=12409-03
- JIJENA, R. Datos personales y consumidores; ojo al cuidador. Diario Financiero en internet, 2021. [En Línea]: https://www.df.cl/noticias/opinion/columnistas/datos-personales-y-consumidores-ojo-al-cuidador/2021-05-05/193731.html
- JIJENA, R. Tratamiento de datos personales en el Estado y acceso a la información pública. *Revista Chilena de Derecho y Tecnología*, Vol. 2 Núm. 2, 2013, pp. 49-94.
- LABBÉ, M. *Big Data:* Nuevos desafíos en materia de libre competencia. *Revista Chilena de Derecho y tecnología,* VOL. 9, Núm. 1, 2020, pp. 33-62.
- LARA, J., VERA, F. y SOTO, B. Privacidad y nuevas tecnologías, regulación chilena y propuestas de política pública. *Policy Paper ONG Derechos Digitales,* N°02, 2013. [En Línea]: https://www.derechosdigitales.org/wp-content/uploads/pp-02.pdf
- MATUS, J. Derecho de acceso a la información pública y protección de datos personales. *Revista Chilena de Derecho y Tecnología*, Vol. 2 Núm. 1, 2013, pp. 197-228.
- MOMBERG, R. y MORALES, M. Las cláusulas relativas al uso y tratamiento de datos personales y el artículo 16 letra g) de la Ley 19.496 sobre Protección de los Derechos

de los Consumidores. *Revista Chilena de Derecho y Tecnología,* Vol. 8 N°2, 2019, pp. 157-180.

- MORALES, S. La Agencia Española de Protección de Datos: Un estudio breve sobre su naturaleza jurídica, su régimen jurídico y su estructura tanto estatal como autonómica. En: *Novum Jus*, V. 14, Núm.2, 2020, pp. 173-194. [En Línea]:https://novumjus.ucatolica.edu.co/article/view/3078

- MAQUEO, M., MORENO, J., RECIO, M. Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de Derecho,* Vol. XXX, N°1, 2017, pp. 77-96.

- NOGUEIRA, H. Autodeterminación informativa y hábeas data en Chile e información comparativa. *Anuario de Derecho Constitucional Latinoamericano*, Universidad Nacional Autónoma de México, Tomo II, 2005, pp. 449-471. [En Línea]: https://revistas-colaboracion.juridicas.unam.mx/index.php/anuario-derecho-constitucional/article/view/30267/27321

- PUENTE, A. La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal. En: *Azpilcueta: cuadernos de derecho*, Núm. 20, 2008, pp.13-41. [En Línea]: https://core.ac.uk/download/pdf/11501783.pdf

- QUEZADA, F. La protección de datos personales en la jurisprudencia del tribunal constitucional de Chile. *Revista Chile de Derecho y tecnología,* VOL. 1, Núm. 1, 2012. pp. 125-147.

- ROSTIÓN, I. Sobre la Ley de Protección de la Vida Privada: La importancia de una "fuente legal" y su aplicación en las personas jurídicas. *Revista Ius et Praxis,* Año 21, N°2, 2015, pp.499-520.

- TALENS, Á. La protección de datos personales como un derecho fundamental en la era de la tecnología y su protección en el ordenamiento jurídico español. Universidad de Jaén, 2019. [En línea]: http://tauja.ujaen.es/bitstream/10953.1/10829/1/TFG_Alvaro_Talens_2805_.pdf

- VERGARA, M. Chile: comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la agencia de protección de datos personales. *Revista Chilena de Derecho y Tecnología,* Vol.6 N°2, 2017, pp.135-152.

NORMATIVA CONSULTADA

NACIONAL:

- BOLETÍN N°11.144-07. REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES.
- BOLETÍN N°12409-03. ESTABLECE MEDIDAS PARA INCENTIVAR LA PROTECCIÓN DE LOS DERECHOS DE LOS CONSUMIDORES.
- BOLETÍN N°6120-07. INTRODUCE MODIFICACIONES LA LEY N° 19.628, SOBRE PROTECCIÓN DE LA VIDA PRIVADA, Y A LA LEY N° 20.285, SOBRE ACCESO A LA INFORMACIÓN PÚBLICA.
- CÓDIGO CIVIL
- CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA.
- LEY N°19. 628 SOBRE PROTECCION DE LA VIDA PRIVADA.
- LEY N° 21096 CONSAGRA EL DERECHO A PROTECCIÓN DE LOS DATOS PERSONALES.

EXTRANJERA:

- *CJI.* INFORME DEL COMITÉ JURÍDICO INTERAMERICANO (CJI) PRINCIPIOS ACTUALIZADOS DEL COMITÉ JURÍDICO INTERAMERICANO SOBRE LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS PERSONALES, CON ANOTACIONES.
- *CONSEJO DE EUROPA.* CONVENIO N°108 PARA LA PROTECCIÓN DE LAS PEROSNAS CON RESPECTO AL TRATAMIENTO AUTOMTIZADO DE DATOS DE CARÁCTER PERSONAL.
- *ESPAÑA.* LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES.
- *ESPAÑA.* REAL DECRETO 428/1993, DE 26 DE MARZO, POR EL QUE SE APRUEBA EL ESTATUTO DE LA AGENCIA DE PROTECCIÓN DE DATOS.

- *UE.* REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 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 Y POR EL QUE SE DEROGA LA DIRECTIVA 95/46/CE (REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS).