UNIVERSIDAD DE CHILE

FACULTAD DE DERECHO

DEPARTAMENTO DE DERECHO PÚBLICO

“ANÁLISIS DESDE LA PERSPECTIVA CONSTITUCIONAL DE LA REGULACIÓN DEL MERCADO DE DATOS EN CHILE”

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

GABRIELLA FRANCISCA BURGOS HERRERA
ISIDORA CECILIA YÁÑEZ GALLARDO
Profesor Guía: Paulino Varas

Santiago, Chile

2019

Agradecimientos:

Al profesor Carlos Isensee Rimassa por su colaboración en este trabajo, el cual no habría sido posible sin su ayuda.

Gabriella e Isidora

Agradecimientos:

A mi familia y amigos por su incondicional apoyo, a Isidora por todo el trabajo realizado y a Dominga, Michelle y Matías por su amor que me acompañará por siempre.

Agradecimientos:

A mi madre, a mi abuela Olga Vicencio.

A Gabriella Burgos, Sofia Acuña Bächler, Constanza Guerrero y a Juan Pablo González.

A Annia Ossandón y a su familia, a Elizabeth Ojeda, y a Alondra Vera Thompson.

A Ignacio Méndez Letelier, a Angel Chiok y a Sergio Herrera Encina

A don Sergio de la Barra, a Daniel Moreno y Winfried Hempel por sus enseñanzas.

TABLA DE CONTENIDO

RESUMEN

El presente trabajo busca analizar el estado actual de la protección de los datos personales y la regulación del mercado en el cual se transan los mismos a la luz de la Constitución Política de la República y la legislación vigente, considerando la reciente modificación al artículo 19 de la Constitución, en su numeral cuarto, el cual consagra dicha protección como un derecho constitucional. En razón de lo anterior, en el primer capítulo se analiza la evolución de la protección de los datos personales como un derecho reconocido expresamente por la Constitución, a partir del concepto de vida privada y la evolución de la protección de la intimidad y privacidad, considerando también la autodeterminación informativa. Luego, en un segundo capítulo, hacemos una revisión de los distintos cuerpos normativos relevantes para la protección de los datos personales y los mecanismos que estos proveen a favor de sus titulares. Finalmente, en el tercer capítulo se analiza el estado actual del mercado en el cual se transan dichos datos personales y su regulación.

INTRODUCCIÓN

Hoy más que nunca en la historia, la información, y en particular aquella referente a las personas es valiosa. Tradicionalmente, en materia económica, se ha entendido que entre más y mejor información tengamos sobre un determinado asunto, mejores decisiones seremos capaces de tomar, maximizando nuestro beneficio, sin embargo los datos personales, es decir, la información referente a una persona identificada o identificable, no son solo una variable a considerar a la hora de analizar cualquier mercado en cual se transe un determinado bien, si no que se trata de un bien en sí misma, que puede ser objeto de transacciones, con un valor propio y que posee una serie de características que lo distinguen de otras clases de bienes y que da origen a un verdadero mercado, en el cual interactúan una serie de actores, públicos y privados en transacciones cuyo valor es inconmensurable.

Por otra parte, debido a la naturaleza de estos datos, se encuentran en juego diversos aspectos jurídicos y sociales, especialmente cuando pueden ser catalogados como “datos sensibles”, lo que ha dado origen a una regulación que considera la protección de los datos personales como un derecho fundamental de sus titulares, los cuales a su vez cuentan con diversas herramientas para su resguardo y que se ha visto profundamente influenciada por las consecuencias del creciente tratamiento automatizado de los datos personales que ha permitido el desarrollo tecnológico.

Dicha regulación se encuentra en constante evolución, principalmente a través de los aportes de la doctrina y jurisprudencia que a partir de las ideas tradicionales respecto a la privacidad, vida privada y honra, entre otros, han permitido configurar las bases para la protección de las personas ante el tratamiento de sus datos.

Es así, como nuestra Constitución en sus primeros textos no contempló el derecho a la protección de datos personales como un derecho fundamental, sino más bien este tuvo como origen el derecho a la privacidad no siendo hasta el año 2018 que

por fin se consagró esta como un derecho protegido constitucionalmente diferenciado del derecho a la privacidad.

Paralelamente, se han desarrollado una serie de principios que orientan la regulación respecto al tratamiento y protección de los datos personales, los cuales serán analizados en el presente trabajo.

Dado lo anterior, el presente trabajo tiene por objetivo analizar ciertos aspectos relevantes del escenario anteriormente descrito, estructurándose en tres capítulos. El primero de ellos, trata sobre la evolución del concepto de protección de los datos personales hasta llegar a ser reconocido como un derecho fundamental en la Constitución.

En efecto, se aborda en primer lugar el concepto de vida privada y como este fue evolucionando a lo largo de la historia constitucional, hasta la redacción actual del artículo 19 N°4. A partir de lo anterior, resulta necesario poder delimitar el concepto de intimidad y privacidad, tanto desde su origen histórico en el derecho comparado como la evolución que tuvo en nuestro país para luego, hacer un recorrido por el concepto de autodeterminación informativa como consecuencia del derecho a la vida privada.

En el segundo capítulo de este trabajo se revisará el concepto de dato personal, sus clasificaciones, así como los principios que rigen su tratamiento y los derechos que asisten a sus titulares en nuestra legislación. De igual manera, repasaremos la actual regulación en la materia en Chile, sus posibles modificaciones y algunos aspectos relevantes de la legislación comparada, así como los procedimientos con los que cuentan los titulares de los datos para ejercer dichos derechos.

Por último, en el tercer capítulo de este trabajo ahondaremos en el mercado de los datos personales, sus características y su regulación, tanto en Chile como en el derecho comparado.

CAPÍTULO I DATOS PERSONALES COMO DERECHO FUNDAMENTAL EN LA CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA.

I. El derecho a la vida privada como Derecho Fundamental

1. El respeto a la vida privada como derecho en la Constitución. Artículo 19 N°4.

Para referirnos a la protección de datos y a su consagración como derecho fundamental en la Constitución, es necesario analizar su origen, contenido esencial y sus límites.

La vida privada y la protección de datos personales son derechos que van estrechamente unidos, ya que no se puede entender el uno sin el otro. El derecho a la protección de la vida privada es un presupuesto de la protección de datos personales y no fue sino hasta el año 2018, que este último se reconoció constitucionalmente en forma explícita. Reforma que por cierto, era necesaria para estar acorde a los tiempos que exigían desde hace ya tiempo un cambio.

El derecho a la privacidad es un derecho de la personalidad que permiten la ejecución de otros derechos, y asimismo funcionan como una base y límite de otras esferas de la vida humana. De modo tal que la Constitución le da protección en cuanto al ejercicio del derecho y a un eventual daño.

Siguiendo a don Hernán Corral[1], el derecho a la privacidad se funda en la dignidad humana. Asimismo, "la esfera de la vida privada como bien jurídico se edifica sobre una realidad de corte antropológico pero es más que ella, ya que se trata de un concepto normativo no puramente descriptivo[2]" de modo tal que ésta debe obedecer a un propósito unificado y no fragmentado. En ese orden de ideas, la privacidad como bien jurídico, "es la posición de una persona (o entidad colectiva personal) en virtud de la cual se encuentra libre de intromisiones o difusiones

[1] CORRAL, Hernán. 2001. El respeto y protección de la vida privada en la Constitución de 1980. [en línea] <https://corraltalciani.files.wordpress.com/2010/04/vida-privada-y-constitucion.pdf >, pág. 2 (Consulta: 06 de enero de 2019).
[2] Loc. Cit.

cognoscitivas de hechos que pertenecen a su interioridad corporal y psicológica o a las relaciones que ella mantiene o ha mantenido con otros, por parte de agentes externos que, sobre la base de una valoración media razonable, son ajenos al contenido y finalidad de dicha interioridad o relaciones[3]".

1.1 El derecho a la intimidad y/o privacidad

Para efectos de este texto, consideraremos intimidad y privacidad como equivalentes, pues, los límites de ambos conceptos están lejos de ser completamente diferenciados el uno del otro y tienen como base fundamentalmente el mismo contenido, así pues, se trata de conceptos que están estrechamente unidos.

El ser humano siempre ha tenido la necesidad de retirarse un momento de la vida pública, para buscar refugio o buscar espacios de recogimiento. Esta necesidad humana de estar consigo mismo, ha ido tomando una necesidad de regulación particularmente más intensa desde la segunda mitad del siglo XX en adelante, aunque el tema de la privacidad, en términos jurídicos comenzó a desarrollarse a finales del siglo XIX, en especial, como ya se ha dicho antes, debido a que las formas de recolección de datos se han multiplicado y hoy por hoy es ilusorio pensar que la tecnología con sus avances no ha vulnerado nuestra privacidad. Sin embargo, el desarrollo doctrinario y jurídico en Chile ha sido débil.

Se ha generado un conflicto entre la libertad de información, por un lado y la honra, la privacidad y la intimidad por otro, pues entendiéndolo como legítimo derecho de que muchos de nuestros asuntos estén exentos del conocimiento de los demás, como un secreto, es de esperar que existan choques entre estos derechos. En su sentido jurídico más originario, "lo privado fue asociado a los llamados derechos de la personalidad, cuyo fundamento es la autoridad que se reconoce a la persona respecto a si misma en sus relaciones con los demás"[4]

[3] CORRAL, Op.Cit. pág. 3.
[4] BARROS BOURIE, Enrique. 1998. Honra, privacidad e información: un crucial conflicto de bienes jurídicos. Revista de Derecho - Universidad Católica del Norte - Sede Coquimbo, pág. 45.

El origen histórico del derecho a la intimidad lo podemos situar con el desarrollo de la burguesía, vinculado al derecho de propiedad, es decir, el ejercicio de la propiedad se entendía estrechamente unido a la aspiración de la privacidad, siendo esta última una extensión del derecho de propiedad, será entonces un privilegio de las altas clases sociales de la época.

Más adelante, fue en el derecho norteamericano donde surge la noción de privacidad o "privacy" o derecho a estar solo "the right to be left alone" el cual "se fundaba esta exigencia de respeto de la intimidad individual contra la intromisión injustificada de su privacidad, proviniera ella no tanto de la acción de otras personas, sino principalmente se le reconocía como una prerrogativa frente a la intromisión del Gobierno en los recintos privados, cualquiera fuesen los medios utilizados"[5]. con un acento especialmente marcado respecto de las irrupciones de la prensa de la época que se encontraba en un auge en cuanto a la injerencia en la vida social de las personas.

El derecho a la privacidad, con la revolución burguesa y los movimientos constitucionalistas, y luego de la segunda guerra mundial adquieren un rango constitucional, siendo integrada en la mayor parte de los Códigos, Constituciones, declaraciones y tratados sobre derechos fundamentales del mundo.

Pues bien, el derecho a la intimidad, en su sentido natural y obvio lo podemos definir como "Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia.[6]" y privacidad se entiende como "Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión[7]" lo que concuerda con lo dicho anteriormente. Además, el derecho a la privacidad e intimidad se encuentra consagrada en el artículo 19 N°4 de la Constitución.

---

[5] BANDA VERGARA, Alfonso. La vida privada e intimidad en la sociedad tecnológica actual y futura. Revista de Derecho Público, (63), págs. 258-278. [en línea] <https://revistaderechopublico.uchile.cl/index.php/RDPU/article/view/36294> (Consulta: 10 de diciembre de 2018).

[6] Real Academia Española de la Lengua RAE, [en línea] <http://dle.rae.es/srv/search?m=30&w=intimidad> (Consulta: 15 de diciembre de 2018)

[7] BANDA, Loc. Cit.

En su aspecto doctrinal, ha sido entendido como un derecho de la personalidad que no puede ser vulnerado por persona o autoridad alguna. Hemos de insistir en este punto que “Vida privada” e “intimidad” están estrechamente vinculados (los consideramos sinónimos), y es un ámbito de la vida del ser humano en que se desarrollan actividades tan importantes como conversar, amar, convivir, compartir alegrías y dolores. Por otro lado, “la sociedad influye enormemente y determina en muchos aspectos al individuo; todo lo cual hace que sea muy importante que el proceso de penetración de la sociedad sobre el hombre tenga un límite que permita a éste formar, consolidar y desarrollar su propia personalidad”.[8]

Ahora bien, el dilema que se suscita en cuanto al derecho a la intimidad tiene que ver con el alcance y el contorno del mismo, es decir, hasta dónde puede determinarse el límite que el derecho tiene para su protección frente a una eventual vulneración. Esto no es fácil de responder y está lejos de determinarse, pues con el avance de la informática y la recopilación de datos que se da segundo a segundo, habrá haber un cambio sustantivo en lo que entendemos por privacidad.

Pero antes que eso, deberíamos revisar qué ha de calificarse como íntimo. Según GARCÍA[9], se han desarrollado varias teorías que sería interesante esbozar:

En primer lugar, se da un criterio espacial o geográfico, en la cual la intimidad tiene que ver con saber cuál es el control que tenemos sobre los objetos materiales, por ejemplo, lo que queda al interior de nuestro hogar es aquello que queda fuera de la intromisión de terceras personas, y si analizamos el texto Constitucional, bien podríamos decir que se extiende a la comunicación epistolar y telefónica, pero este criterio tiene el problema de ser restringido, pues sólo tiene en cuenta cuestiones externas, por ejemplo, si estuviéramos en el Metro de Santiago, no habría siquiera un espacio de privacidad (por ejemplo, cualquiera podría entrometerse en nuestras conversaciones telefónicas o de WhatsApp) y

[8] AROS CHIA, Rodrigo Marcelo. 2001. El derecho a la intimidad frente a la sociedad de información. Revista de Derecho de la Universidad Católica de Valparaíso XXII. Pág. 210 y 211.
[9] Véase GARCÍA, Luis. 1992. Reflexiones sobre la intimidad como límite de la libertad de expresión. En: Estudios sobre el derecho a la intimidad. Madrid, Editorial Tecnos. pp. 15-35.

“minusvalora la trascendencia social de las conductas desplegadas por las personas en el medio[10]” y no podría proteger intromisiones de larga distancia, como cámaras de seguridad.

En segundo lugar, dentro de las concepciones subjetivas, la intimidad tiene su límite en determinar si una persona es un personaje público y funcionario público, o una persona normal cualquiera (y sin ninguna exposición social como las mencionadas primero), atendiendo a la naturaleza de sus funciones o por la influencia que alcance su actuar, tanto un personaje público y un funcionario público en estricto rigor no tendrían derecho a la intimidad. Esta distinción también se ha discutido en el derecho administrativo, desde el punto de vista de la probidad administrativa (discusión que podemos afirmar que está zanjada), sin embargo, llevado al ámbito de la protección de datos personales y de la intimidad en particular, parece lógico descartar esta distinción, pues no precisa la extensión de la intimidad (además de ser ridícula) y tampoco goza de criterio de igualdad jurídica “ya que admite la privación del derecho a los funcionarios y personajes públicos con independencia de la relevancia de su comportamiento[11]”

En tercer lugar, es de un punto de vista objetivo, dejando de lado consideraciones materiales o que se fundan en la calidad que detentan ciertas personas, se puede hacer una distinción entre las conductas públicas o privadas. Son conductas privadas “aquellas desplegadas con el propósito de satisfacer necesidades propias: en cambio, las conductas públicas, aquellas que han tenido por finalidad satisfacer necesidades ajenas[12]” las primeras quedarían protegidas por el derecho a la intimidad y las segundas no. Pues bien, según CERDA, esta distinción parece ser demasiado rígida, pues para distinguir entre una y otra habría que verificar la trascendencia a que puede estar sujeta la conducta del sujeto.

[10] CERDA SILVA, Alberto. 2003. Autodeterminación informativa y leyes sobre protección de datos. Revista Chilena de Derecho Informático, N°3, pág. 2.
[11] Ibíd.
[12] Ibíd.

Pese a lo dicho anteriormente, la doctrina apunta a que la determinación de lo que es íntimo o privado es esencialmente casuístico.

Pero por otro lado, y dentro del ámbito de la doctrina norteamericana, el Profesor Charles Fried, el núcleo duro del derecho a la intimidad tiene que ver con el control que tenemos sobre la información acerca de nosotros mismos[13] la privacidad "expresa un poder para excluir a personas no autorizadas del conocimiento de hechos que quedan bajo el control exclusivo de cada cual[14]" de modo tal que la privacidad tiene una doble faz, es decir, por un lado es un límite a la intromisión de terceros y por otro que se difundan hechos relativos al ámbito privado. Intromisión versus divulgación.

Por último, si hablamos específicamente de internet, fenómeno que ha generado los cambios más significativos de fines del siglo XX y principios del XXI, hay que precisar si internet es o no un medio de comunicación social, y la verdad es que no lo es "puesto que no cumple con los caracteres propios de un medio de comunicación social de aquellos señalados por la Constitución y las leyes, toda vez que Internet carece de un editor o director responsable en contra del cual puedan dirigirse aquellas personas que consideren que han sido violentados[15]" Internet es un medio tecnológico que comparten todos.

1.2 La autodeterminación informativa

Con todo lo dicho anteriormente, hemos de entender que el tratamiento de datos personales, el derecho a la privacidad y/o intimidad y otros derechos fundamentales puedan verse seriamente afectados (y de hecho es así) pues Internet y otros medios permiten disponer de información de otros a un bajo costo y fácil acceso y de los cuales se tiene legítimo derecho a tener resguardado.

Las funciones del Estado de hoy en día no sería posible sin el tratamiento de datos personales, así como diversas funciones llevadas a cabo por agentes privados,

[13] BARROS, Op. Cit. pág. 46.
[14] BARROS, Loc.Cit.
[15] AROS, Op.Cit, pág. 212.

pero éstas siempre deben tener como finalidad un bien mayor. El desarrollo de la telemática entendido como un enlace entre las telecomunicaciones con la informática es una serie de servicios de naturaleza informática.

Recordemos además que es a través de esta concepción moderna del derecho a la vida privada que la doctrina ha desarrollado el concepto de un derecho a la "autodeterminación informativa", el cual igualmente cuenta con una dimensión negativa que permite al titular impedir intromisiones no deseadas por parte de terceros y una dimensión "activa y dinámica consistente en la prerrogativa de conocer, acceder y por supuesto controlar el flujo de informaciones concernientes a la persona."[16]

El derecho a la autodeterminación informativa, en este sentido "se constituye a partir del derecho a la intimidad, tanto como éste lo hizo sobre la base del derecho de propiedad; y, en que, a diferencia de cuanto ocurre con el derecho a la intimidad, la autodeterminación informativa no se circunscribe a amparar a la persona frente al tratamiento de datos personales que le conciernan y que revelen circunstancias personales que merezcan permanecer en la esfera privada, sino que, en general, se extiende a todo dato que se predica de determinada persona[17]"

La libertad informática se puede considerar como una nueva disciplina jurídica, pues se han multiplicado los intereses económicos y jurídicos vinculados al desarrollo informático y al aumento de la información constantemente, de modo tal que esto alcanza los intereses del Estado, y entre Estados, y obviamente a intereses económicos privados, ya que ha generado una nueva forma de riqueza y poder en una nueva dimensión.

Volviendo al derecho a la intimidad, este último debe ser considerado como principio básico de todo Estado democrático "en donde el respeto por la vida privada de las personas, y su honor, no solo debe enmarcarse o entenderse en el

[16] Op. Cit. pág. 270 y 271.
[17] CERDA, Op.Cit. pág. 3.

contexto de las relaciones íntimas de las personas y de su familia, sino también, proyectarse en el campo de las opiniones políticas[18]".

2. Origen constitucional del derecho a la vida privada.

2.1 Antecedentes previos e historia del artículo 19 N°4.

Pues bien, el artículo 19 N°4 de la Constitución de 1980 (previo a la reforma constitucional del año 2018) asegura "El respeto y protección a la vida privada y a la honra de la persona y su familia" y más adelante el N°5 reza lo siguiente "la inviolabilidad del hogar y de toda forma de comunicación privada" ligando la privacidad un sentido espacial.

Sin embargo, en la Constitución no se define la noción de vida privada (ni en la ley tampoco) trabajo que quedó dado a la jurisprudencia y la doctrina. Asimismo, la protección de datos personales también estuvo largo tiempo sin consagración directa como derecho fundamental, sin perjuicio de su débil protección legal.

En las constituciones previas a la de 1980 entendía la protección de la privacidad limitada a la inviolabilidad del hogar y la correspondencia, es decir, circunscrita netamente a la comunicación epistolar. Así, el Reglamento Constitucional de 1812 garantizaba la seguridad de sus personas, casas, efectos y papeles (artículo 16 de la Constitución de 1812) sin darle un alcance demasiado extenso.

Luego, al Constitución de 1833 hablaba en forma más sencilla de la "casa" a la que declara "asilo inviolable". Se excepcionaba el caso de allanamiento por motivo señalado en la ley y en virtud de orden de autoridad[19].

Más tarde en la Constitución de 1925 la norma fue reproducida casi sin cambios, asegurando a los habitantes "la inviolabilidad del hogar. La casa de toda persona que habita en el territorio chileno sólo puede ser allanada por motivo especial determinado por la ley y en virtud de orden de autoridad competente" (artículo 10

[18] Ibíd.
[19] CERDA, Op. Cit.pág. 4.

N°12) y en cuanto a la inviolabilidad de la correspondencia, incluyó la correspondencia telegráfica (ya protegía la comunicación epistolar).

El derecho a la vida privada se vio casi inalterado durante largo tiempo, tanto en su aspecto normativo constitucional como desarrollo jurisprudencial y doctrinario. Fue después de la segunda mitad del siglo XX cuando comienza a darse un desarrollo más profundo al concepto del derecho a la vida privada, pues con el desarrollo de la tecnología se vieron desarrollados nuevos derechos fundamentales, entre ellos, la privacidad.

El origen de los artículos 19 N°4 y N°5 fue introducido por don Alejandro Silva Bascuñán, quien integró parte de la Comisión de Estudios de la Nueva Constitución, y quien pensó en la intimidad como protección contra la sociedad masificada, pues quiso proteger los valores superiores del individuo. Así pues fue que instauró como una garantía, basándose en las constituciones más modernas.

La primera redacción del artículo 19 N°4 rezaba "...El respeto a la intimidad y al honor de la persona y de su familia, y la inviolabilidad y de la correspondencia cualquiera que sea el medio por el que esta se realice

El hogar sólo podrá allanarse o la correspondencia abrirse, interceptarse o registrarse en virtud de orden de autoridad competente, fundada en un motivo especial determinado por la ley[20]"

Sin embargo, Jaime Guzmán, propuso su consagración como "El respeto a la privacidad y a la honra de las personas" expresando que sería mejor el concepto de "privacidad" que "vida privada". Luego, el comisionado Jorge Ovalle propuso "El respeto y protección de su vida privada, de su honra y la de su familia".

Luego, como proyecto aprobado por la Comisión, se propuso la siguiente redacción "El respeto y protección a la vida privada y a la honra de la persona y de su familia; la inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados

[20] CORRAL, Op.Cit. pág. 7.

interceptarse, abrirse, o registrarse, en los casos y formas determinados por la ley”

El proyecto del Consejo de Estado finalmente separó la protección de la vida privada y la honra y la inviolabilidad del hogar y la correspondencia, pero agregó la expresión “vida pública”, quedando lo siguiente “El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia.

Si la infracción de este precepto se cometiere a través de un medio de comunicación social y consistiere en la imputación de un hecho o acto falso o que cause injustificadamente daño o descrédito a una persona o a su familia, será constitutivo de delito a menos que el medio de comunicación social a requerimiento del ofendido y salvo que se trate de injurias cometidos en perjuicio de particulares, pruebe la verdad de la imputación. Además, los propietarios, editores, directores y administradores del medio serán solidariamente responsables de las indemnizaciones que procedan[21]”

Sin embargo, la norma fue modificada nuevamente, quitando la expresión “a la vida privada y pública y a la honra”

Así las cosas, la norma quedó como sigue “El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia.

La infracción de este precepto, cometida a través de un medio de comunicación social, y que consistiere en la imputación de un hecho o acto falso, o que cause injustificadamente daño o descrédito a una persona o a su familia, será constitutiva de delito y tendrá la sanción que determine la ley. Con todo, el medio de comunicación social podrá excepcionarse probando ante el tribunal correspondiente la verdad de la imputación, a menos que ella constituya por sí misma el delito de injuria a particulares. además, los propietarios, editores, directores y administradores del medio de comunicación social respectivo serán solidariamente responsables de las indemnizaciones que procedan”

[21] CORRAL, Op.Cit. pág. 8 y 9.

Finalmente, en el año 2005 se llevó a cabo una reforma al artículo 19 N° 4 mediante la ley 20.050 en el cual se suprimió todo el inciso segundo, quedando como conocimos dicho artículo hasta la reforma del año 2018 “b) Sustitúyase el número 4º, por el siguiente:

"El respeto y protección a la vida privada y a la honra de la persona y su familia."

2.2 El derecho a la vida privada desde el punto de vista constitucional

Como vimos anteriormente, en principio se agruparon los conceptos vida privada, vida pública y honra en un solo precepto. Siguiendo a Hernán Corral, lo anterior podría dar pie a preguntarse si todos estos conceptos constituyen un sólo derecho o si, por el contrario son distintos. Se entendió en todo caso que estos conceptos fueron reunidos por una cuestión práctica, ya que al ser vulnerada la intimidad, usualmente se vulneraría la honra de una persona.

Así las cosas, la protección a que se refiere el artículo 19 N°5 sobre la inviolabilidad del hogar, de las comunicaciones y documentos privados debe entenderse como una especificación al derecho y protección a la vida privada.

Ahora bien, en cuanto a la naturaleza jurídica del derecho a la vida privada, Silva Bascuñán lo entendía como derecho individual en contraposición a los derechos sociales, ya que estos últimos serían correspondientes a los grupos sociales y no al individuo. Sin embargo, y aunque la redacción del artículo 19 N°4 no contiene la palabra “derecho” el derecho a la vida privada se encuentra en el Capítulo III de la Constitución De los Derechos y deberes Constitucionales, y aunque otros derechos (valga la redundancia) como el derecho a la vida o a la educación si contienen dicha palabra, no habría razón para no entender el derecho a la vida privada como un derecho fundamental. Sin embargo “es claro que en la enumeración del artículo 19 hay derechos constitucionales propiamente tales (con carácter de derecho subjetivo por su concreción y exigibilidad inmediata) y otras

libertades o aspiraciones sociales que no llegan a ser derechos propiamente tales (aunque puedan ser fuente de ellos)[22]"

Asimismo, el respeto y protección de la vida privada es una imposición que se dirige a toda persona, natural o jurídica, instituciones, grupos, al poder público, al Estado y a los tribunales, tanto en un sentido pasivo y activo. El Estado debe respetar, proteger y promover su protección, ya que, como señala el artículo 5 de la Constitución "es deber de los órganos del Estado respetar y promover tales derechos, garantizados por ésta Constitución, así como por los tratados internacionales ratificados por Chile y que se encuentran vigentes" en términos tales que el ejercicio de la soberanía reconoce como limitación el respeto a los derechos esenciales que emanan de la naturaleza humana.

2.3 Distinción entre vida privada y vida pública

La primera redacción del artículo 19 N°4 contemplaba la voz "vida pública" como objeto de protección, la cual fue suprimida posteriormente. Sin embargo, cabe preguntarse por qué esta inclusión en la norma, y qué diferencia merece la protección de una u otra.

Siguiendo a Hernán Corral, se proponen varias alternativas. La primera de ellas dice relación con que tanto la vida pública como la vida privada tienen el mismo tratamiento, es decir, deben tener el mismo respeto, promoción y protección. Se rechaza esta tesis pues, sería una negación a la vida privada, la cual tiene importancia justamente porque se opone a la vida pública, es decir que necesariamente todo sería vida pública.

Otra opción propuesta es que, al referirse al concepto de vida pública, el Constituyente se refirió al respeto a personas que tienen relevancia pública. Esta interpretación tiene origen en el resquemor que tenía el expresidente Jorge Alessandri respecto de la necesidad de prevenir el posible abuso por parte de la prensa sobre personas que ostentaran una relevancia de esa naturaleza. Sin

[22] CORRAL, Op.Cit. pág. 11.

embargo, parece obvio que no podemos aceptar esta interpretación, pues no se ha dado a entender en qué consistiría esta protección a la vida pública de ciertas personas. Por otro lado, el derecho vulnerado en este caso sería cuestión del derecho a la honra, y a su vez, el derecho otorga otras herramientas para casos en que se vea vulnerado este, la difamación no pone en juego el derecho a la vida privada.

El derecho a la vida pública, en la Constitución se entiende como un derecho de toda persona a que la imagen y apariencia que ella exhibe ante el público, así como los aspectos visibles definitorios de su personalidad, no sean utilizados o distorsionados por terceros[23].

2.4 Persona y familia

La expresión "familia" a la que alude el artículo 19 N°4 de la Constitución en relación a la honra, ligado a su vez a la honra de las personas fallecidas tiene su razón de ser. La familia es la comunidad básica de la sociedad, y también está protegida por la constitución y por ende debe tener una protección específica. La familia debe conectarse con el derecho a la honra, y necesariamente al derecho a la vida privada, ya que "de lo absurdo que sería el reservar el valor de la institución familiar sólo para la honra y no para la intimidad, y por último de la misma intención del Constituyente[24]." Así las cosas, la vida familiar también debe ser respetada por los demás y su vulneración debe ser sancionada. De modo tal que el constituyente quiso ligar la protección de la familia a la vida privada.

2.5 Derecho a la vida privada en relación al artículo 19 N°5

Como ya se ha mencionado anteriormente, el artículo 19 N°5 asegura "La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley" tiene una estrecha relación con la protección de la vida privada, y también marca un límite

[23] CORRAL, Op.Cit. pág. 15.
[24] CORRAL, Op. Cit. 16.

en relación con aquellas cosas que deben permanecer en secreto e intimidad, es decir, el artículo 19 N°5 sería una extensión externa de la protección a la vida privada.

Derecho que por cierto debe ser considerado inherente a la persona humana, y respeto por los órganos del Estado.

La honra puede entenderse como un concepto objetivo, pues podemos entenderlo como "la autoestima, a la consideración o, quien sabe, si al orgullo que cada cual tiene de sí mismo[25]" "la buena fama, el crédito, prestigio o reputación de que una persona goza en el ambiente social, es decir, ante el prójimo o los terceros en general[26]". En este sentido, la honra se encuentra unida a la dignidad de la persona y a su naturaleza psíquica, siendo este un derecho personalísimo. así, la honra de una persona es su apreciación por los demás, lo que debe ser protegido por el derecho.

Por último, el concepto de honor y honra se considera como sinónimo, Alejandro Silva Bascuñán entiende que "honra y honor son expresiones analógicas, y en que presentan una dualidad de significados: subjetivo y objetivo[27]", aunque hay voces que consideran que el honor conllevaría un concepto más moralista, sin embargo, no ahondaremos en esto por no ser materia de este trabajo.

2.6 Recepción constitucional de los Tratados Internacionales.

La primera vez que el derecho a la vida privada tuvo lugar cuando Chile ratificó el Pacto Internacional de Derechos Civiles y Políticos, pacto que entró en vigencia en el año 1976 pero recién fue publicado en el Diario Oficial en el año 1989, pasando 13 largos años.

Pues bien, en el artículo 17 del Pacto se protege la vida privada en los siguientes términos "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida

[25] CEA EGAÑA, José Luis. 2012. Derecho Constitucional Chileno, Tomo II, Editorial Universidad Católica de Chile, pág. 180.
[26] CEA, Op. Cit. pág. 201.
[27] SILVA BASCUÑÁN, Alejandro. 2003. Tratado de Derecho Constitucional Tomo XI. Santiago, Editorial Jurídica, pág. 193.

privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."

Así también en la Convención sobre los Derechos del Niño, que fue publicada en el Diario Oficial en el año 1900, su artículo 16 habla en los mismos términos, a saber "1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación. 2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques."

Por otra parte, la Convención Americana sobre Derechos Humanos (Pacto San José de Costa Rica) publicado en el Diario Oficial en el año 1991 en su artículo 11 también protege la privacidad en términos similares, sobre la protección de la honra y la dignidad indica que "1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."

Además de lo señalado en los acápites anteriores, Chile es miembro de una serie de organizaciones internacionales, las cuales incluyen estándares en cuanto a la protección de los datos personales, algunas de las más relevantes son:

1) Organización para la Cooperación y el Desarrollo Económico (OCDE): El Ingreso de Chile a la OCDE obliga al Estado a adecuar nuestra normativa en privacidad y protección de datos a sus Directrices sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales. Actualmente, tal compromiso no se ha cumplido, lo que le ha valido al país advertencias de parte de la Organización respecto al incumplimiento de los acuerdos adoptados para aceptar su incorporación al grupo.

2) Organización de Estados Americanos: Actualmente se encuentra en elaboración una Ley Modelo Interamericana sobre Protección de Datos Personales.

3) Foro de Cooperación Económica Asia-Pacífico (APEC): En 2004 se adoptó un Marco con Principios sobre Privacidad, y se ha buscado desarrollar reglas de privacidad transfronterizas para transferencia de información personal entre miembros en materias de negocios.

4) Red Iberoamericana de Protección de Datos (RIPD): Originada luego del Encuentro Iberoamericano de Protección de Datos de 2003, busca fomentar el avance de la regulación en la materia en la región.

En definitiva, los tratados internacionales son obligatorios en virtud del artículo 5 de la Constitución, por lo que constituyen leyes en el derecho interno y con lo mencionado anteriormente se desprende que la norma del artículo 19 N°4 ya desarrollada se enriquece con las normas de los tratados internacionales. Por tanto, el derecho a la privacidad es un derecho protegido tanto constitucional como internacionalmente.

II. Respeto y protección de la vida privada y protección de datos personales: una reforma necesaria al artículo 19 N°4 de la Constitución.

En el mismo orden de ideas, la protección de datos personales no tenía una protección explícita en materia constitucional, sino que solo quedaba resguardada el derecho a la privacidad. Asimismo, con el pasar de los años y el desarrollo de un mundo globalizado tuvo como consecuencia la creación de nuevas tecnologías.

No es difícil advertir que con internet nuestro mundo se desarrolló a niveles jamás vistos por la humanidad, y el derecho tuvo que hacer frente a este nuevo desarrollo. En particular, nuestro país tuvo modificaciones insignificantes para la

protección de la privacidad y un escaso desarrollo jurisprudencia en torno a la protección de datos propiamente tal.

Con todo, en el año 2018 se modificó la Constitución, elevando la protección de datos personales a un rango constitucional. La iniciativa tuvo lugar gracias a Felipe Harboe, Pedro Araya, Ricardo Lagos Weber, Hernán Larraín y Eugenio Tuma. Quienes tuvieron en consideración las recomendaciones realizadas por la OCDE. La aprobación en el Senado resultó por unanimidad tras las modificaciones introducidas por la Cámara de Diputados la que posteriormente fue promulgada.

Según el Boletín N°9.384-07 de fecha 17 de enero de 2018 reconoce justamente que el uso, tratamiento, comunicación y almacenamiento de la información requería de un cambio. Para ello se tomó en cuenta la legislación de Estados Unidos (privacy of autonomy) y la Unión Europea, algunos países como Alemania, España y América Latina. Se habla de la privacidad como derecho fundamental ligado intrínsecamente a la protección de datos, indicando que la información personal debe estar siempre bajo el control de su titular, protegiéndolo de la intromisión ilegítima de terceros.

Con todo, consideramos que esta modificación recoge la idea desarrollada por la doctrina de que la intimidad contendría un aspecto negativo “en cuanto el individuo ante los demás, se encierra en sí mismo excluyendo del conocimiento foráneo algunos aspectos personales que desea mantener ocultos, de un aspecto positivo**,** en cuanto tiene una facultad de control de los datos e informaciones relativos a su persona” [28].

En palabras de Harboe “Este proyecto constituye un momento histórico y no es exageración, toda vez que vamos a consagrar en la Constitución un nuevo derecho para todos los ciudadanos (…). Según la OCDE en los últimos 5 años, el uso de internet en la Región aumentó un 55% y según CEPAL en un segundo se descargan 1700 aplicaciones, 2 millones de correos y hay 50 mil publicaciones en

[28] BANDA, Op. Cit. pág. 265.

Facebook[29]". Por otro lado, Pérez Varela señaló que "Incluso el 2015 la OCDE le representó a Chile el retraso en su normativa de protección de datos; en su minuto se dijo que entre sus miembros solo Chile y Turquía no han perfeccionado en nada su legislación (…). La Cámara mejoró sustancialmente su redacción, según especialistas esta modificación busca el concepto al derecho de las personas a controlar sus datos personales, incluso si estos no se refieren a su intimidad[30]". Por último, Letelier expresó que "Este proyecto tiene tremenda importancia (…) La Comisión de Transportes profundizó este debate. En la era del Big Data además es importante el cómo se accede a los datos y cómo se utilizan para otro fin, por ello la importancia de que no se puedan interceptar las comunicaciones. (…) Estos son temas de época[31]" con lo que se deja en claro que la reforma Constitucional tenía la finalidad de una protección más óptima de los datos personales.

Pues bien, el antiguo texto constitucional fue reemplazado por el siguiente: "4º.- El respeto y protección a la vida privada y a la honra de la persona y su familia, *y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley;* "

Será cosa de tiempo ver los resultados o si dicha reforma fue útil tarea que quedará para la doctrina y la jurisprudencia.

III. Conclusiones

La Constitución en sus primeros textos no contempló el derecho a la protección de datos personales como un derecho fundamental, sino más bien este tuvo como origen el derecho a la privacidad. Asimismo, la privacidad fue desarrollado por el derecho en forma paulatina como necesidad de la revolución burguesa y el derecho norteamericano.

---

[29] Protección a los datos personales como derecho constitucional será una realidad. [en línea] http://www.senado.cl/proteccion-a-los-datos-personales-como-derecho-constitucional-sera-una/senado/2018-05-15/181511.html (Consulta: 19 de enero de 2019).
[30] Ibíd.
[31] Ibíd.

Así las cosas, la doctrina y la jurisprudencia fueron desarrollando un concepto de privacidad (y también el derecho a la honra, la persona, familia e inviolabilidad de las comunicaciones), en particular en Chile esta se reguló desde muy temprano en la Constitución y en lo que se refiere a protección de datos personales se fue tornando más intenso su desarrollo desde la segunda mitad del siglo XX. Con todo, no fue sino hasta el año 2018 que por fin se consagró como un Derecho Fundamental protegido constitucionalmente, diferenciándose del derecho a la privacidad.

CAPÍTULO II: LOS DATOS PERSONALES Y SU PROTECCIÓN

I. Los datos personales

1. Concepto de datos personales

Estamos en la era de la información y del conocimiento, lo que ha traído una transformación de la sociedad por completo. La tecnología es parte de nuestra vida diaria, ya que desarrollamos nuestras actividades con ella, consumimos productos y servicios y nos relacionamos con una diversidad de entidades, es decir, personas naturales, empresas, instituciones, gobiernos.

En la Ley N°19.628 sobre protección de la vida privada, podemos encontrar varias definiciones que van perfilando el concepto de protección de datos personales. Así, en palabras de Alberto Cerda, el concepto "dato" es una "unidad básica de información (...) cuando la información que porta el dato es relativa a una persona determinada o susceptible de serlo, se denomina dato personal o dato nominativo, esto es, una unidad de información que se predica de persona determinada o determinable[32]"

Luego, la Ley N°19.628 en su artículo 2° define dato personal o datos personales como "son aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables" es decir, que los datos personales son los relativos a cualquier persona naturales, identificadas o identificables, sea que se trate de información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo[33]. Y cuando se dice "toda información" quiere decir que el concepto de dato personal es amplio y no distingue por naturaleza ni por soporte

[32] CERDA SILVA. Alberto. 2012. Legislación sobre protección de las personas frente al tratamiento de datos personales. Apuntes de clases, Centro de Estudios de Derecho Informático. Universidad de Chile. pág. 16

[33] Consejo para la Transparencia. Recomendaciones del consejo para la transparencia sobre protección de datos personales por parte de los órganos de la administración del Estado. Santiago, 5 de septiembre de 2011. [en línea] <http://200.91.44.244/transparencia_activa/mecanismos/propuesta_de_recomendacion_pd_general_version_consulta_publica_11abril2011.pdf,> pág 2, (Consulta: 30 de junio de 2018).

que contiene dicha información, puede ser una imagen, sonido, y puede manifestarse de múltiples formas.

Los elementos básicos que constituyen una definición de datos personales son los siguientes:

1- Debe tratarse de información relativa a una persona, siendo indiferente la naturaleza del dato, antecedente o hecho de que se trate.

2- Debe tratarse de información que permita identificar al titular. Es decir, la información puede indicar ya sea en forma directa o indirecta de la persona en concreto de quien se trata, por ejemplo, el RUT, domicilio o teléfono. Por tanto, si para identificar a una persona se requiere una actividad de naturaleza excesivamente compleja o no permite su identificación, no se considerará dato personal.

3- El titular sólo puede ser una persona natural. Ya que nuestra legislación ampara la protección de la vida privada en torno a personas naturales y no jurídicas. Sin perjuicio de ello, existen países que sí lo protegen. Sin embargo, en el caso chileno, serán sólo personas naturales.

Asimismo, podemos ejemplificar a modo meramente ilustrativo que los datos personales son, nombre, edad, sexo, RUT, estado civil, profesión, domicilio, números de teléfono, e-mail, números de cuentas bancarias, etc.

Las leyes de protección de datos - En Chile y derecho comparado- han definido a los datos personales en términos bastante generales, de tal forma que, cualquier información concerniente a una persona debe ser a lo menos determinable. Según Paula Jervis la amplitud del término “facilita su adaptación a la constante evolución de la tecnología y la informática, utilizando el principio de neutralidad tecnológica;

no limita el concepto solamente a información escrita, sino que también la imagen, la voz, las huellas digitales constituyen datos personales[34]"

La Directiva Europea 95/46/CE, -hoy reemplazada por el nuevo Reglamento Europeo de Protección de Datos- en su artículo 2 letra a), entendía como dato personal como "toda información sobre una persona física identificada o identificable (el "interesado); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

Sin embargo, luego de largas negociaciones entre países miembros de la Unión Europea, que entró en vigencia el 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), entiende actualmente en su Artículo 5 letra f) que los Datos de carácter personal como "Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables."

En Estados Unidos, por otro lado, no existe una regulación orgánica respecto de la protección de datos personales, sino que se trata de una regulación sectorial.

Dicho esto, a contrario sensu, podemos señalar que un dato no es personal:

1- Cuando la información simplemente no es sobre un ser humano

2- Cuando la información si bien se refiere a un ser humano, es anónima.

[34] JERVIS, Paula. 2006. La regulación del mercado de datos personales en Chile. Tesis para optar al grado de Magíster en Derecho. Santiago, Universidad de Chile, Facultad de Derecho de la Universidad de Chile, pág. 46.

3- Cuando la información es directamente identificable a un grupo y sólo indirectamente identificable a los individuos que componen ese grupo[35]

Sin perjuicio de la definición de datos personales, hay que reconocer que este fenómeno va de la mano con lo que se conoce como la autodeterminación informativa, lo que en definitiva significa tener control sobre nuestros datos y el derecho a saber sobre la información, archivos y ficheros registros de información personal, públicos o privados. Asimismo, quienes tienen esos datos y por lo demás el derecho a actualizarlos o solicitar rectificación o cancelación, a través del hábeas data o bien, a través del recurso (acción) de protección principalmente.

2. Clasificación o categorías de datos personales.

Los datos personales, admite diversas clasificaciones, dentro de las cuales podemos destacar, principalmente y sin perjuicio de otras categorías, las siguientes:

2.1 A la luz de la propia Ley N°19.628

1.1) Dato personal o datos personales "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables" Artículo 2° letra f).

1.2) Datos sensibles: "aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual" Artículo 2° letra g).

1.3) Dato estadístico: "el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable. Este último queda, por tanto, fuera del ámbito de aplicación de la ley". Artículo 2° letra e).

[35] JERVIS, Op.Cit. pág. 47.

1.4) Dato caduco: “aquel que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna”. Artículo 2° letra d).

2.2 Datos personales directos e indirectos.

2.1) Directos: Son aquellos que provienen de la voluntad de su titular, quien ha entregado información de manera voluntaria.

2.2) Indirectos: Aquellos que no se obtuvieron a partir de la voluntad misma del titular de datos, sino a través o desde una base de datos, ya por transmisión, cesión, interconexión o algún mecanismo equivalente

2.3 Datos personales sensibles y no sensibles.

1) Datos sensibles: Como ya definimos más arriba, los datos sensibles son “aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual” Artículo 2° letra g) de la Ley N°19.628. Estos datos deberán ser especialmente resguardados, ya que podrían eventualmente dar pie a discriminaciones arbitrarias. Asimismo, la ley es más rigurosa al momento de tratar este tipo de datos, protegiéndolos con mayor intensidad.

2) Dato no sensible: A contrario sensu, son aquellos que no revisten de las características anteriores y que en la mayoría de los casos no requiere consentimiento previo para su tratamiento u obtención.

2.4 Datos públicos y datos no públicos.

1) Datos públicos: Se refiere a datos personales de acceso público, es decir, aquellos datos personales a los cuales puede acceder cualquier interesado, como por ejemplo, censos, bases de datos del Registro Civil, jurisprudencia, etc.

2) Datos no públicos: Aquellos a los cuales se les aplica algún grado más o menos intenso de restricción al público.

3. Principios que rigen el tratamiento de datos personales y derechos de los titulares.

En la rama de la protección de los datos personales podemos encontrar principios que nos sirven como orientación y parámetros base que constituyen un determinado ámbito del saber, estos principios guían la legislación y en este caso también sirven como base mínima para la protección de datos personales.

Los principios que orientan la protección de datos personales han sido dados por los organismos internacionales en la materia, tales como la Organización de Cooperación y Desarrollo Económico a través de su "recomendación relativa a las directrices aplicables a la protección de la vida privada y a los flujos transfronterizos de datos personales", la cual fue adoptada por el Consejo de ministros de dicha organización el 23 de septiembre de 1980, el Consejo de Europa con la #recomendación de la Comisión 81/670/CEE relativa al Convenio del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal" de 29 de julio de 1981[36]".

Asimismo, Las Naciones Unidas a través de los "principios rectores para la reglamentación de los ficheros computarizados de datos personales" adoptado por la Asamblea General de las Naciones Unidas en su resolución 45/95 de 14 de diciembre de 1990.

Dichos principios rigen tanto para el Estado y sus organismos, y también para el tratamiento de datos efectuado por privados. Siguiendo principalmente a VIOLLIER[37], los mencionados principios son los siguientes:

[36] JERVIS, Op.Cit. pág. 63.
[37] VIOLLIER, Pablo. 2017. El Estado de la protección de datos personales en Chile. Informe realizado por Derechos Digitales [en línea] <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf> (Consulta: 4 de marzo de 2018).

3.1 Libertad en el tratamiento de datos personales.

La misma ley señala que “toda persona puede efectuar el tratamiento de datos personales” en el artículo 1° de la Ley N° 16.628, por lo que, podemos señalar que es evidente que la ley no prohíbe el tratamiento de datos personales.

Sin perjuicio de lo anterior, el límite que reconoce la les es que el tratamiento debe ser acorde a la legislación, con la finalidad permitidas por la ley y que no sea contrario a los derechos fundamentales de los titulares.

3.2 Información y consentimiento del titular.

El principio de información de los titulares de datos personales, dice relación con el derecho de autodeterminación informativa, es decir, el derecho de cada persona a controlar su propia información. De tal forma que “dicha persona debe ser informada sobre el propósito del almacenamiento de sus datos y su eventual publicación, y la autorización debe realizarse en forma expresa y por escrito[38]” como señala el artículo 4° de la ley, asimismo, la autorización puede ser revocada sin expresión de causa.

Podemos ver también, que en artículo 3° de la Ley 19.628, que cuando se recopilen datos personales realizados a través de encuestas, estudios de mercados, etc., se debe informar a las personas sobre el propósito para el cual se solicita dicha información

En relación al principio consentimiento del titular de datos, se establece éste como la regla general, ya que se requiere de un consentimiento expreso, libre y voluntario para el tratamiento de sus datos.

Sin embargo, este principio tiene excepciones que, tal como se verá son tan amplias que fácticamente la regla se invierte:

Las excepciones son:

[38] VIOLLIER, Op.Cit. pág. 21.

i- Datos obtenidos de fuentes accesibles al público: dichos datos pueden ser objeto de tratamiento sin consentimiento del titular, y como señala el artículo 2° i) de la Ley N°19.628 son “los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes”

ii- Tratamiento por personas jurídicas privadas: cuando son para su uso exclusivo y la de sus afiliados.

iii- Tratamiento por organismo públicos: aunque debe tratarse de materias del organismo correspondiente.

3.3 Principio de finalidad.

Este principio tiene su origen en el artículo 9° de la Ley N°19.628 “los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados”, que en definitiva se traduce en expresar las razones por las cuales se recolectan dichos datos y quedar limitado al cumplimiento de dicha finalidad y no otras, de modo que se configura como uno de los más importantes y se extiende a otros principios.

Así, el objetivo de un banco de datos debe ser específico, y no debe usarse con un propósito incompatible, y se encuentra ligado con el principio de consentimiento e información.

3.4 Protección especial de los datos sensibles.

Tal como señalamos en otro momento, los datos sensibles son aquellos que se refieren a características específicas de las personas, como físicas o morales, religiosas, ideologías, opiniones políticas, etc. La ley intensifica la protección de este tipo de datos porque son aquellos que afectan más fácilmente a los Derechos Fundamentales.

Es por esto que el legislador lo prohibió, salvo tres excepciones “(i) que la ley lo autorice (ii) que exista consentimiento del titular, o (iii) que dichos datos sean

necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares[39]"

3.5 Seguridad de los datos

Este principio dice relación con que deben tomarse todas las medidas necesarias para que los bancos de datos y sus correspondientes datos personales sean destruidos de manera accidental o sin su autorización, o su modificación, acceso de forma irregular.

Como podemos observar, el artículo 11 de la Ley N° 19.628 establece la obligación del responsable del banco de datos de cuidar de ellos, haciéndose responsable por los daños, cabe observar que como la ley no da un estándar de cuidado, son los tribunales quienes deben determinar, caso a caso si se ha dado cumplimiento a este deber.[40]

3.6 Deber de secreto

Según el artículo 7° de la Ley N°19.628 "Las personas que trabajan en el tratamiento de datos personales, tanto en organismo públicos como privados, están obligados a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo."

En definitiva, acorde al mencionado artículo, se debe reservar y fijar todas aquellas medidas tendientes a proteger los datos personales por riesgo que puedan afectar por acciones de terceros que pongan en peligro y puedan perjudicar a los titulares de los datos.

[39] VIOLLIER, Op.Cit. pág. 23.
[40] ibíd.

3.7 Calidad de los datos personales.

Este principio dice relación con que los datos personales que sean tratados deben ser adecuados, exactos y pertinentes durante toda la fase de su tratamiento. Esto quiere decir que los datos también deben ser los más completos posibles para evitar errores.

Asimismo, este principio se relaciona estrechamente con el principio de veracidad (los datos deben ser veraces en relación a la situación fáctica del individuo), con el principio de finalidad ya descrito anteriormente y con el principio de proporcionalidad (recabar solo datos necesarios).

4. Derechos de los titulares de datos

Así como la ley permite el tratamiento de datos personales, también establece una serie de derechos que permiten a los titulares solicitar su modificación, rectificación, eliminación y bloqueo de sus datos, así como también el derecho de accionar a través del habeas data y otras acciones. Estos derechos se encuentran principalmente, en el Título II de la Ley N° 19.628.

Por otro lado, en materia de tratamiento de datos personales por parte del Estado, y "conforme al artículo 12 de la Ley N°19.628, pueden ejercer respecto de los órganos de la Administración del Estado, los derechos que se describen en este numeral, teniendo presente las características de independencia, gratuidad y sencillez[41]"

Cabe mencionar que los derechos de los titulares no pueden ser limitados por ningún acto o convención, conforme al artículo 13 de la ley en comento. De esta manera, cualquier cláusula, acto, convención, contrato, declaración de voluntad unilateral, que esté destinada a limitar o a suprimir el ejercicio de estos derechos

[41] Recomendaciones del Consejo para Transparencia sobre protección de datos personales por parte de los órganos de la administración del Estado. Santiago, 5 de septiembre de 2011, pág. 7.

será nula absolutamente por objeto ilícito, en relación con el artículo 10 del Código Civil, que señala que los actos prohibidos por la ley son nulos y de ningún valor[42].

4.1 Derecho de información o acceso.

Se refiere a que toda persona puede exigir del responsable del banco de datos, la información que estos posean sobre ellas, así como el origen del mismo, su objetivo o su destinatario. Así como señala el artículo 12 de la Ley N°19.628 "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"

Por otro lado, el artículo 22 de la Ley N°19.628 indica que "El Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos" Asimismo, indica que este registro de banco de datos será público y constará el fundamento jurídico de su existencia, su finalidad y tipos de datos almacenados y descripción del universo de personas que comprende.

Cabe señalar que el referido artículo 22, no se extiende a entidades privadas "quedando estas últimas exentas de la obligación de registrar sus bases de datos, y mermando con ello la capacidad de las personas naturales de ejercer su derecho de información y acceso[43]"

Así pues, el derecho a la información reviste de importancia por el hecho de que sin este derecho no podrían ejercerse los demás, ya que en principio necesitamos saber quiénes, cómo, cuándo y por qué el tratamiento de los datos personales de los titulares.

[42] JERVIS, Op.Cit., pág. 137.
[43] VIOLLIER, Op.Cit. pág. 25.

4.2 Derecho de modificación o rectificación

En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen (artículo 12 de la Ley N°19.628 inciso 2°)

Así, el titular de datos que requiere la modificación de sus datos personales deberá acreditar esta circunstancia, y podrá ejercerse dicho derecho toda vez que un dato personal no corresponda a la realidad actual de la persona.

4.3 Derecho de cancelación eliminación

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 (artículo 12 de la Ley N°19.628 inciso 3°)

Así, la eliminación de datos personales debe entenderse en los términos del artículo 2° letra h) como “eliminación o cancelación de datos, la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello”

4.4 Derecho de bloqueo

El derecho de bloqueo se entiende como “la suspensión temporal de cualquier operación de tratamiento de los datos almacenados” art 2° Letra b) Ley 19.628.

Este derecho se puede ejercer cuando el titular que haya entregado voluntariamente sus datos personales o cuando se usen sus datos para comunicaciones informativas, y asimismo el titular de datos no quiera seguir en el registro respectivo de manera temporal o definitiva, o también, cuando los datos personales del titular no sean exactos.

Este derecho procede, además, cuando no corresponda la cancelación, es decir, procede en forma subsidiaria a ella.

4.5 Derecho a accionar

Aun cuando hemos revisado anteriormente los derechos que otorga a los titulares de datos personales, el ordenamiento jurídico otorga algunas acciones judiciales en caso de que se afecten los derechos de los titulares.

De modo tal que los titulares de datos personales han de recurrir a los tribunales ordinarios a través de la acción de protección o a través del habeas data, para hacer efectivo sus derechos y poder resguardarse de terceros, acciones que trataremos en un apartado más adelante, con el fin de explicarlos en mayor profundidad.

Cabe señalar que, sin perjuicio de las acciones de los titulares de datos personales, los costos asociados a la tramitación judicial, sumado al relativo desconocimiento que sufren los individuos del tratamiento que terceras personas realizan de sus datos personales, hacen que la carencia de una autoridad de control afecte directamente la aplicabilidad de la Ley 19.628 para los ciudadanos comunes[44].

Asimismo, la Ley N°20.285 del año 2008 otorga al Consejo para la Transparencia el deber de velar por el debido cumplimiento de la Ley N°19.628, por parte de los órganos de la Administración del Estado.

Aunque el Consejo realiza recomendaciones para la adecuada protección de datos personales a los Órganos de la Administración del Estado, este no cuenta con la facultad de sancionar el incumplimiento o la vulneración de los derechos de los titulares de datos personales tanto a los Órganos de la Administración del Estado como a entidades privadas.

[44] VIOLLIER, Op.Cit. pág. 27.

II. Regulación de la protección de los datos personales

1. Descripción general

Ya sea que se hayan planteado el desafío de regular la protección de los datos personales de sus nacionales en forma consciente y sistemática, o bien haya sido simplemente el resultado de una serie de acontecimientos externos, prácticamente todos los Estados tienen algún cuerpo normativo que en alguna medida se ocupe de ello, y por supuesto, más allá de los reparos que pueda merecer nuestra legislación, Chile no es la excepción.

Siguiendo a Jervis, "es posible intentar una clasificación de las leyes de protección de datos en leyes omnicomprensivas (como la chilena) y leyes sectoriales. Las primeras aplican al tratamiento de datos que efectúe cualquier entidad, tanto pública como privada y respecto a cualquier tipo de dato"[45], mientras que las segundas, son leyes que regulan específicos tratamientos de datos.

Lo anterior es el resultado de la adopción de uno de los dos grandes modelos de regulación en la materia: la impulsada por la Unión Europea y aquella propia de los Estados Unidos de América, respectivamente.

1.2 Derecho comparado

La masificación de los procedimientos automatizados de tratamiento de la información en los años 70, despertó el interés en configurar un marco normativo para la misma, dictándose la primera ley sobre el tema en la República Federal Alemana (conocida como "Datenschutz"), dando origen entonces a una tendencia en el resto de Europa, que llevó hasta la entrada en vigencia en 1981 del Convenio de Estrasburgo del Consejo de Europa cuyo fin era garantizar el derecho de las personas a la vida privada con respecto al tratamiento automatizado de sus datos personales, dicho convenio fue eventualmente reemplazado por la Directiva 95/46 /CE de 1995, la cual fuere el gran referente mundial en materia de regulación de la protección de los datos personales, y que fue complementada con instrumentos

[45] JERVIS, Op.Cit. pág 53.

posteriores en pos de lograr la uniformidad y generalidad de la regulación en toda la Unión Europea, hasta finalmente ser reemplazada por el Reglamento General de Protección de Datos, cuya aplicación comenzó en mayo de 2018 y al cual dedicaremos un apartado posterior en este trabajo.

Por otra parte, tal como se señalaba, la regulación en los Estados Unidos es esencialmente sectorial, por lo que se encuentra contenida en un sinnúmero de leyes que abarcan a su vez diversas materias y territorios, considerando las particularidades de la organización federal norteamericana, por lo que fue necesario en su momento el establecimiento de principios comunes que posibilitaran la transferencia de datos personales desde la Unión Europea a los Estados Unidos. El resultado de tales esfuerzos fueron los llamados “Principios de Puerto Seguro”, los cuales han sido adoptados por o han influenciado el tratamiento regulatorio de distintos países, sin perjuicio de ya encontrarse superados por la actual regulación comunitaria.

1.2.1 España

El caso español es reconocido por la robustez de su regulación en la materia, guiada por la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD), del 13 de diciembre de 1999, la cual dio origen a la Agencia Española de Protección de Datos, con el objeto de velar por su cumplimiento.

Además de la AEPD, en consideración a las particulares administrativas de España, existen agencias especiales en las comunidades autónomas de Cataluña y País Vasco.

Gracias a que la AEPD es considerada un órgano independiente y a que cuenta con, entre otras, facultades de prevención, fiscalización y sancionatorias, es que ha logrado establecerse como una de las entidades más activas en la materia

1.2.2 Alemania

Alemania se ha caracterizado por estar siempre a la vanguardia legislativa respecto a la protección de los datos personales, generando la primera ley en la

materia en los años 70, y más recientemente con la dictación en 2017 de la nueva Ley alemana de Protección de Datos (Bundesdatenschutzgesetz), la cual es la primera de su especie en adaptarse al nuevo Reglamento General de Protección de Datos.

1.2.3 Latinoamérica

A diferencia de la unión europea, Latinoamérica no cuenta con un modelo generalizado para la protección de los datos personales, por lo que cada país ha desarrollado su propia normativa en la materia, generalmente influenciados por el modelo europeo.

De acuerdo con lo previsto en la ya superada Directiva 95/46 del Parlamento Europeo y del Consejo, en la región solo Argentina y Uruguay fueron declarados países con adecuado nivel de protección, en los años 2003 y 2012 respectivamente, a efectos de autorizar la transferencia de datos personales desde Europa hacia ellos.

1.3 Protección de los datos personales en Chile

1.3.1 Descripción general del marco normativo.

En el caso de Chile, podemos decir, en una primera instancia, que nuestra legislación se basa, o al menos toma cierta inspiración, en el modelo europeo, sin embargo, es fácil advertir que sus diferencias, pues es ciertamente menos comprensiva, carece de un órgano de control y, dado el panorama global actual y el uso masivo de las tecnologías de la información en el tratamiento de los datos personales, se encuentra enormemente desactualizada.

Actualmente, la protección de los datos personales y su tratamiento se encuentra contenida en los siguientes cuerpos normativos:

1.3.2 Constitución Política de la República

A partir de la publicación de la Ley 21.096 en junio de 2018, la Constitución Política de la República consagró por primera vez en forma explícita el derecho a la

protección de los datos personales. La señalada ley modificó el Artículo 19 de la Carta Fundamental en su numeral 4.

Esta modificación al texto constitucional viene a confirmar los planteamientos de diversos autores quienes consideraban posible extraer a partir de diversos preceptos constitucionales, principalmente del antiguo texto del artículo 19 N°4 el cual consagra “el respeto y protección a la vida privada y pública y a la honra de la persona y de su familia,” sumado a los numerales 5, que trata de la inviolabilidad del hogar y de toda forma de comunicación privada, y 26 que complementa esta protección en el sentido de que no se podrá afectar la esencia de este derecho o impedir su libre ejercicio, pautas normativas respecto a la materia, al establecer que los datos personales forman parte de la esfera privada de las personas.

Por otra parte, el artículo 5 de la Constitución obliga a respetar los derechos garantizados por los tratados internacionales ratificados por Chile, los cuales igualmente consagran los derechos señalados anteriormente y para los cuales resultan igualmente aplicables las consideraciones doctrinarias señaladas. Entre los más importantes se encuentran La Declaración Universal de Derechos Humanos (1948), El Pacto Internacional de Derechos Civiles y Políticos (1966) y la Convención Americana de Derechos Humanos (1962) entre otros, todo lo cual ha sido desarrollado con mayor detalle en el Capítulo I de este texto.

1.3.3 Organizaciones e Instrumentos Internacionales

Además de lo señalado en los acápites anteriores, Chile es miembro de una serie de organizaciones internacionales, las cuales incluyen estándares en cuanto a la protección de los datos personales, y al igual que el punto anterior han sido desarrollados en la primera parte de este texto.

1.3.4 Leyes sectoriales

En nuestro ordenamiento jurídico existen variadas normas sectoriales que dentro de su articulado regulan materias relacionadas con la protección de los datos personales, algunas de las más relevantes son:

a) Ley 17.336 sobre Propiedad Intelectual, especialmente en su artículo 3°, número 17, que trata sobre la protección de las bases de datos.

b) Ley 19.496 Sobre protección de los derechos de los consumidores, la cual trata el tema del “spam” en su artículo 28 B.

c) Ley 19.970 que Crea el sistema nacional de registro de ADN.

d) Ley 20.285 sobre Acceso a la información pública, la cual consagra el deber del Consejo para la Transparencia de velar por la protección de los datos en su artículo 33.

1.3.5 Ley Sobre Protección de la Vida Privada

La Ley 19.628 sobre protección de la vida privada, publicada en 1999, es la norma dedicada específicamente el tratamiento de datos personales, el funcionamiento de las bases de datos, los derechos y deberes de los involucrados y un mecanismo de solución de controversias, siendo la primera ley de esta clase de América Latina, sin perjuicio de que en el proyecto original se buscaba dar un estatuto de protección a la vida privada en general.

Si bien a lo largo de este trabajo hemos analizado las disposiciones de dicha ley en diversos apartados, a modo de resumen podemos decir que esta cuenta con un: (i) Título Preliminar, en el que se contienen disposiciones de carácter general y definiciones; (ii) Título I. De la Utilización de Datos Personales; (iii) Título II. De los Derechos de los Titulares de los Datos; (iv) Título III. De la Utilización de Datos Personales Relativos a Obligaciones de Carácter Económico, Financiero, Bancario o Comercial; (v) Título IV. Del Tratamiento de Datos por Organismos Públicos; (vi) Título V. De la Responsabilidad por las Infracciones a esta Ley; y (vii) Título Final el cual añade modificaciones al Código Sanitario referida a datos médicos. Además, incluye una serie de disposiciones transitorias.

Así es que la ley regula, en primer lugar, su ámbito de aplicación y establece el principio de que toda persona puede efectuar tratamiento de datos personales,

siempre y cuando este sea hecho en forma concordante con ella. Otras disposiciones relevantes de la misma son, por ejemplo, las definiciones contenidas en su artículo 2, algunas de las cuales ya han sido comentadas en este trabajo, las hipótesis en las cuales puede realizarse el tratamiento de datos personales por parte de los particulares o los organismos públicos, la posibilidad de que estos sean transmitidos y las condiciones para ellos. Así como los principios que informan el tratamiento, los derechos de los titulares de los datos y el procedimiento para hacerlos valer.

En cuanto a las iniciativas legislativas que han modificado su texto original, y han configurado la actual Ley 19.628, encontramos las leyes números 19.812, del año 2002, 20.463 del año 2010, 20.521 del 2011 y finalmente la 20.575 del 2012. Igualmente más adelante en este trabajo dedicaremos algunas palabras a los proyectos de ley sobre el tema más relevantes actualmente en tramitación en el Congreso.

Esta ley ha sido objeto de diversas críticas. Entre estas se encuentran: la falta de una autoridad de control en la materia, la nula regulación de las transferencias transfronterizas de datos, la falta de sanciones robustas para quienes infrinjan sus disposiciones y el establecimiento de un procedimiento de poca aplicación práctica, entre otras.

1.3.6 Proyectos de ley y reformas pendientes a la Ley 19.628

Ante las ya mencionadas críticas hechas a Nuestra Ley 19.628 h, y a los avances que ha tenido la regulación comparada, han surgido una serie de proyectos para su modificación. Actualmente, los boletines N°11.144-07 y N°11.092-07, refundidos, configuran el proyecto que, todo indica, modificará en definitiva esta ley. A continuación, revisaremos someramente dicho proyecto en cuanto a sus planteamientos más importantes:

En cuanto a su ámbito de aplicación, este indica que “todo” tratamiento que no esté regido por una ley especial, se regirá por las disposiciones de dicha normativa, por

lo que tendrá aplicación supletoria a la regulación especial. De igual modo, el proyecto establece que se excluirán ciertos tratamientos de datos personales de la aplicación de la ley, a saber: (i) el tratamiento de datos que realicen los medios de comunicación social en el ejercicio de las libertades de emitir opinión y de informar, reguladas por las leyes a que se refiere el artículo 19 N°12 de la Constitución Política de la República y (ii) el tratamiento que efectúen las personas naturales en relación con sus actividades personales.

El proyecto de ley modifica y agrega una serie de nuevas definiciones a la lista establecida en la Ley N°19.628, tales como: “comunicación o transmisión de datos personales”, “dato personal”, “dato personal sensible”, “fuentes de acceso público”, “proceso de anonimización o disociación”, “base de datos personales”, “responsable de datos”, “titular de datos”, “tratamiento de datos” y “consentimiento”, así como la definición de los derechos que poseen los titulares de los datos.

Por otra parte, el proyecto establece como principios que regirán el tratamiento de los datos personales los de “licitud del tratamiento”, “finalidad”, “proporcionalidad”, “calidad”, “responsabilidad”, “seguridad” e “información”.

En cuanto a los derechos de los titulares de los datos personales, el proyecto establece que estos serán: i) “acceso”; ii) “rectificación”; iii) “cancelación”; iv) “oposición”); y v) “portabilidad”, mientras que, el inciso segundo del artículo 15 ter del proyecto, al momento de la redacción de este trabajo, establece un sexto derecho “a no ser sujeto a decisiones individuales automatizadas”.

Estos derechos deben ser ejercidos directamente ante el responsable del tratamiento, y ante la negativa de la solicitud específica basada en el derecho ejercido, el titular de los datos puede acudir a la Agencia de Protección de Datos Personales, creada por el mismo proyecto.

En cuanto a las condiciones para el tratamiento de los datos personales, el proyecto establece como regla general, el consentimiento del titular. Dicho

consentimiento no será necesario: i) cuando los datos han sido obtenidos de fuentes de acceso público y su tratamiento esté relacionado con los fines para los cuales fueron entregados o recogidos; ii) cuando el tratamiento esté referido a datos relativos a obligaciones de carácter económico, financiero, bancario o comercial y se realice respetando las normas específicas sobre tratamiento de esa categoría de datos; iii) cuando el tratamiento sea necesario para el cumplimiento de una obligación legal; iv) cuando el tratamiento sea necesario para la ejecución de un contrato en que es parte el titular; v) cuando el tratamiento sea necesario para la satisfacción de intereses legítimos del responsable o de un tercero, siempre que no se afecten derechos y libertades fundamentales del titular; y, vi) cuando el tratamiento de datos lo disponga la ley.

El proyecto de ley, a su vez, permite la cesión de datos personales, siempre que se cuente con el consentimiento del titular de datos o lo autorice la ley.

En cuanto a los datos personales de carácter sensible, la regla general de acuerdo al proyecto es que para su tratamiento se requiere del consentimiento expreso del titular, sea escrito, verbal o por medio tecnológico equivalente. Para el caso de los datos personales relativos a la salud, se requiere además que el tratamiento sea: i) necesario para el diagnóstico de una enfermedad o la determinación de un tratamiento; ii) cuando exista urgencia médica o sanitaria; iii) cuando se deba calificar el grado de dependencia o discapacidad de una persona; iv) cuando resulte indispensable para la ejecución o cumplimiento de un contrato cuyo objetivo o finalidad exija tratar datos relativos a la salud del titular; v) cuando sean utilizados con fines históricos, estadísticos o científicos, para estudios o investigaciones de interés público o beneficio de la salud humana, o para desarrollar productos o insumos médicos que no podrían desarrollarse de otra manera. Respecto a los datos personales biométricos, para poder realizar el tratamiento se debe además informar sobre i) el sistema biométrico utilizado; ii) la finalidad; iii) período de uso de los datos; iv) forma en que pueden ejercerse derechos respecto de este tratamiento. Por último, se establece que para el tratamiento de los datos personales relativos al perfil biológico humano, este debe

hacer, para alguno de estos fines: i) realizar diagnósticos médicos; ii) prestar asistencia médica o sanitaria de urgencia; iii) realizar estudios o investigaciones científicas, médicas o epidemiológicas en beneficio de la salud humana o investigaciones antropológicas, arqueológicas o de medicina forense; iv) cumplir resoluciones judiciales.

El proyecto introduce además “categorías especiales de datos personales”, sin que por ello sean considerados datos sensibles y que cuentan con reglas específicas para su tratamiento, estos son: los datos personales relativos a niños, niñas y adolescentes; los datos personales con fines históricos, estadísticos, científicos y de estudios o investigaciones; y los datos de geolocalización.

Un punto relevante del proyecto es que regula la transferencia internacional de datos personales, estableciendo sus requisitos y presupuestos, cuestión no tratada en la ley vigente.

Por otra parte, el proyecto crea la Agencia de Protección de Datos Personales, organismo que estará en manos del Consejo Para la Transparencia y que estará dotado de amplias facultades fiscalizadoras relativas a las obligaciones consagradas en la nueva normativa y ante el cual los titulares de los datos podrán hacer valer sus derechos, erigiéndose como la autoridad de control en la materia.

Finalmente, el proyecto de ley establece una serie de infracciones y sanciones y da la posibilidad a las empresas de que establezcan modelos de prevención aprobados por la autoridad de control.

1.3.7 Decretos y Reglamentos

Finalmente vale la pena destacar algunos reglamentos, tales como el Decreto 779/200 del Ministerio de Justicia que aprueba el reglamento del registro de datos personales a cargo de organismos públicos creado por la Ley Sobre Protección de la Vida Privada y el del Consejo Para la Transparencia.

2. Jurisprudencia en Chile y Procedimientos para la protección de los derechos de los titulares de datos de datos personales

2.1 Tribunal Constitucional.

El Tribunal Constitucional no se ha quedado ajeno a la discusión que desarrollamos en estas páginas respecto a la protección de datos personales. En el proceso del desarrollo de la jurisprudencia del TC podemos identificar dos etapas.

En principio, el TC no otorga una relevancia de rango constitucional a la protección de datos.

Se ha constatado que la tecnología es fundamental para el desarrollo de cualquier tarea diaria y para el desarrollo de la industria, el comercio y el Estado la tecnología hace que todo el mercado sea posible. Ahora bien, corremos el peligro que del uso de la tecnología sea mal usado, y por ello se debe asegurar el uso democrático de la información y la tecnología.

Siguiendo a Flavio Quezada, el problema es propiamente constitucional en un doble sentido. “Primero, en las sociedades desarrolladas científica y técnicamente las insospechadas posibilidades de reunir, almacenar, relacionar y transmitir todo tipo de información permite que bien los poderes públicos, bien los sujetos privados, puedan tener conocimiento de amplias parcelas de nuestras vidas y puedan utilizar dicha información para su beneficio (no necesariamente) notorios daños[46]” y en segundo lugar, bien es sabido que la información es poder, y en especial porque permite influir en las decisiones de las personas, por ello, la limitación del poder es fundamental para el resguardo del derecho. El fundamento se radica en la protección de la esfera íntima del ser humano como expresión de la privacidad y la democracia en su conjunto.

[46] QUEZADA RODRIGUEZ, Flavio. 2012. La protección de datos personales en la jurisprudencia del Tribunal Constitucional de Chile. Revista chilena de derecho y tecnología. Centro de estudios en derecho informático. Universidad de Chile. Issn 0719-2576 vol. 1 nro. 1, pág. 127.

El Tribunal Constitucional se ha referido en diversas ocasiones al derecho resguardado por el artículo 19 N°4 de la Constitución Política. En una primera etapa, se verifica una ausencia de la protección de datos personales en términos constitucionales.

El primer fallo de esta materia en comento, rol N°198-94 de 4 de enero de 1995 es el primer pronunciamiento referido a la vida privada y a la honra de toda persona y su familia, pero que no trató el tema desde el punto de vista de protección de datos personales directamente, en gran medida porque los términos “intimidad” y “privacidad” son tomados como iguales o equivalentes.

El fallo del TC se dicta a raíz de las potestades del Consejo de Defensa del Estado de solicitar a diversas instituciones públicas y privadas el envío de antecedentes, documentos, información financiera con el fin de acumular antecedentes probatorios. El TC consideró que “Que el referido inciso tercero del artículo 16 del proyecto vulnera la Constitución al no proteger el goce efectivo de los derechos y libertades que la Carta asegura y garantiza a todas las personas, cuando dota a un servicio público, Consejo de Defensa del Estado, de facultades absolutamente discrecionales, como las de recoger e incautar documentos o antecedentes probatorios de cualquier naturaleza pertenecientes a personas objeto de una investigación de dicho servicio, o para requerir a terceros la entrega de antecedentes o documentos sobre cuentas corrientes bancarias, depósitos u otras operaciones sujetas a secreto o reserva pertenecientes también a las personas investigadas”

En relación a lo anterior, se infringe la garantía del artículo 19 N°5 en relación con el N°4 de la Constitución “lo que la doctrina ha denominado el derecho a la intimidad de que gozan las personas y su familia” al no contemplar en forma íntegra, completa y exacta los procedimientos ni casos aplicables, porque se refiere a situaciones absolutamente discrecionales en los que deben actuar los funcionarios autorizados para recopilar e incautar documentos, antecedentes y objetos. Es decir, que se vulnera la inviolabilidad de las comunicaciones y documentos privados que solo pueden interceptarse en los casos y formas que

señala la ley. Con lo dicho anteriormente se comienza a consagrar el principio de la legalidad de la protección de datos personales.

En otra sentencia Rol N°389-03 dictada con fecha 28 de octubre de 2003 a propósito del proyecto de ley que crea la unidad de análisis financiero y modifica el código penal en materia de lavado y blanqueo de activos, se trata más en concreto el elemento de la privacidad aplicable a la protección de datos personales, aunque no se refiere de manera explícita a ello. Lo que se indica en dicho fallo es que al atribuirle a la Unidad de Análisis Financiero la facultad de solicitar información sin limitación vulnera el derecho a la privacidad y dignidad humana.

Señala en el considerando decimoctavo que "la Carta Fundamental asegura a todas las personas, sin distinción ni exclusión alguna, en su artículo 19 Nº4 inciso primero, "El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia." En tal sentido considera esta Magistratura necesario realzar la relación sustancial, clara y directa, que existe entre la dignidad de la persona, por una parte, y su proyección inmediata en la vida privada de ella y de su familia, por otra, circunstancia que vuelve indispensable cautelar, mediante el respeto y la protección debidas, ese ámbito reservado de la vida, en el cual no es lícito penetrar sin el consentimiento del afectado, de un lado, o por decisión de la autoridad fundada en la ley que hubiere sido dictada con sujeción a la Constitución, de otro[47]"

Cuando nos referimos al principio del consentimiento, recordemos que este el título que justifica el tratamiento de datos. Además, la sentencia señala que los sujetos que están obligados a la protección del artículo 19 N°4 son tanto el legislador como los particulares.

Luego, en el considerando vigésimo primero indica que "Que el respeto y protección de la dignidad y de los derechos a la privacidad de la vida y de las comunicaciones, son base esencial del desarrollo libre de la personalidad de cada

[47] Sentencia Rol N°389-03 del Tribunal Constitucional de fecha 28 de octubre de 2003.

sujeto, así como de su manifestación en la comunidad a través de los grupos intermedios autónomos con que se estructura la sociedad. En ligamen con lo que viene de ser expuesto, menester resulta recordar que tal autonomía es también sustento del sistema de instituciones vigente en nuestro país, debiendo a su respecto cumplirse la exigencia de respeto, especialmente cuidadoso, que se ha destacado ya con relación a la dignidad de la persona humana"

Sin embargo, la vida privada es un derecho que puede ser limitado, siempre que sea dentro de los márgenes que determina la Constitución, en el sentido de no vulnerar el contenido esencial de este derecho.

Otra sentencia a considerar en esta primera etapa del TC en relación a la protección de datos personales, es la causa Rol N°1365-09 dictada con fecha 8 de abril del año 2010, que tuvo su origen en un requerimiento de inaplicabilidad por inconstitucionalidad de los artículos 5º, 6º, 16, 17, 18 y 1º transitorio, inciso segundo, de la Ley Nº19.970, que crea el Sistema Nacional de Registros de ADN. Al respecto, el TC analiza la constitucionalidad de la toma de muestras biológicas (forzada) a una persona condenada para obtener una huella genética.

En esta ocasión, el TC parece ser tibio en cuanto a un análisis más profundo sobre la protección de datos personales, más bien en este caso a la protección de datos sensibles. Aunque indica que "que la privacidad, en sus variados rubros, por integrar los derechos personalísimos o del patrimonio moral de cada individuo, merecen reconocimiento y protección excepcionalmente categóricos tanto por la ley como también por los actos de autoridad y las conductas de particulares o las estipulaciones celebrados entre éstos[48]" .

Cabe considerar que el razonamiento que hizo el TC en este caso es que, como este registro de ADN no permite indagar sobre otras características de la persona más que la identidad de la misma y el registro que sólo puede consultar el Ministerio Público, tribunales u organismos autorizados. Asimismo, existe un

[48]Sentencia Rol N°1365-09 del Tribunal Constitucional de fecha 08 de abril del 2010, considerando vigésimo,

deber de reserva sobre la información allí contenida “la privacidad estaría legítimamente limitada, por cuanto se afecta en forma precisa y determinada mediante una ley que persigue objetivos legítimos[49].”

Ahora bien, en una segunda etapa, se integra definitivamente la protección de datos personales al ámbito constitucional, la que se puede visualizar a partir del año 2011.

Con la sentencia Rol N°1732-10-INA y rol N°1800-10-INA (acumulados) dictada con fecha 21 de junio del año 2011, que tuvo como origen un recurso de inaplicabilidad por inconstitucionalidad entre TVN y el Consejo para la transparencia, en el sentido de la aplicación del deber de transparencia activa en las empresas pública y la publicación de remuneraciones de sus funcionarios y ejecutivos.

Los requirentes del rol N°1732-10 (Ejecutivos de TVN) sostienen que TVN infringiría el derecho a la privacidad dispuesto en el artículo 19 N°4 de la Constitución cuando se ha revelado información confidencial relativa a sus remuneraciones. Por otro lado, el requirente de la causa Rol N°1800-10 alega que la aplicación de los 16 preceptos que reprocha a los gerentes de área de TVN sería inconstitucional, pues no se cumpliría en tal caso la finalidad prevista por el legislador al establecer el deber de transparencia activa tratándose de TVN y, consecuencialmente, se infringiría el artículo 19, Nº2° y Nº21°, de la Constitución, en relación con el estatuto[50].

En la sentencia en comento, el TC considera que “el artículo 19, N°4°, de la Constitución, además del derecho al honor y a la honra, asegura a todas las personas el respeto y la protección de la vida privada, el cual debe quedar al amparo de la injerencia de terceras personas. La Constitución procura facilitar así el pleno ejercicio de la libertad personal sin interferencias ni intromisiones o presiones indebidas. Así lo establece claramente, por su parte, el artículo 11, N°2,

[49] QUEZADA, Op.Cit. pág. 135
[50] Sentencia Rol N°1732-10-INA y rol N°1800-10-INA (acumulados) de fecha 21 de junio del año 2011 del Tribunal Constitucional, considerando sexto.

de la Convención Americana de Derechos Humanos: “Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada… Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques”; de modo tal que se reconoce expresamente la relación entre la protección de datos personales y la vida privada (y de paso el derecho a la autodeterminación informativa).

El derecho a la autodeterminación informativa implica que las personas puedan conocer la existencia de datos personales contenidos en ficheros o bancos de datos, sean públicos o privados, la finalidad y responsables de los bancos de datos de manera que las personas que estén en ellas puedan conocer los datos que los bancos contienen, y teniendo derecho de pedir su recolección, conservación, actualizar o rectificar.

Según QUEZADA, por primera vez se asume la protección de datos personales como un problema genuinamente constitucional, asentando su protección en el ámbito normativo de la vida privada[51]. sin embargo, señala, que el TC entiende en términos negativos la protección de la vida privada y a la vez, un ámbito de su regulación como un derecho de autodeterminación. Asimismo, considera que la vida privada, amparada constitucionalmente, se delimita en un principio de no lesión de intereses sociales o derechos fundamentales, “dado el rango constitucional de la protección de datos personales, la delimitación que hagan los intereses sociales ha de ser amparada en normas de igual rango, por lo mismo, solo puede ser restringido o delimitado por derechos de igual jerarquía[52]”.

Se reconoce por el TC que no todos los datos son sensibles, pero que todos merecen protección desde el artículo 19 N°4, es decir, que tanto los datos personales y los datos sensibles (como subcategoría de datos personales) gozan de igual rango normativo, pero que el legislador ha de proteger los datos sensibles con mayor intensidad.

[51] QUEZADA, Op. Cit., pág. 138
[52] QUEZADA. Op. Cit., pág. 139.

Por último, vale traer a la vista la sentencia rol N°1894-2011 de fecha 12 de julio del año 2011 dictada por el Tribunal Constitucional, dictada a propósito de la constitucionalidad de un registro privado a cargo de un cibercafé (o centros de acceso a internet), en especial cuando se está frente a cibercrimen.

Al respecto, el TC analiza la situación de que, por un lado permitir el seguimiento de usuarios que utilizan cibercafés sean monitoreados constantemente, produciría un desincentivo a este tipo de negocios, sustituyéndolos por otros oferentes, asimismo, el considerar que cada persona que utiliza este tipo de negocios sería sospechoso de algún crimen.

Así, dentro del contexto del artículo 19 N°4 de la Constitución en relación al Pacto Internacional de Derechos Civiles y Políticos, cuyo artículo 17 que indica "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada" y que "2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques", lo que implica que nadie sea objeto de acechos.

De modo tal que el conflicto es atingente directamente a la protección de la vida privada, en cuanto al monitoreo constante implica una injerencia a la intimidad personal, por cuanto agentes públicos o privados pueden recopilar información personal. Porque el monitoreo constante permite revelar preferencias personales, opciones comerciales e inclinaciones sociales de las personas.

Por otra parte, el TC "vuelve a reiterar la doctrina de la privacidad/libertad-negativa, se deja abierta la posibilidad de ampliar el contenido de esta garantía constitucional[53].

Se da la situación de que la intimidad no solo se verifica en lugares privados sino también en algunas circunstancias en espacios públicos, como es el caso de los cibercafés y en internet.

Por último, siguiendo a QUEZADA, deben establecerse garantías de protección adecuadas o suficientes para resguardar la vida privada, las que deben ser

[53] QUEZADA, Op. Cit., pág. 142.

establecidas legalmente, siendo inconstitucional una remisión global en blanco al reglamento[54].

2.2 Tribunales Ordinarios

Para la defensa de los datos personales, sus titulares han hecho uso de diversas estrategias procesales para obtener el amparo sus derechos mediante la actuación de los Tribunales del país, ya sea en forma directa o accesoria a una petición principal.

2.3 Habeas data

Hemos visto que existe regulación en materia de protección de datos personales a través de la Ley N°19.628 y el artículo 19° N°4 de la Constitución, principalmente, que protegen la vida privada y los datos personales.

La sociedad de la información y el desarrollo de la telemática no han impedido el tratamiento de datos, los cuales se llevan a cabo día a día, y que ha sido fundamental para el desarrollo de la industria, y sin embargo, las personas ven afectados sus derechos pues no ha sido posible que todos tengan conocimiento de qué es lo que se hace con sus datos personales que circulan por el mercado.

Antes de la Ley N°19.628 sobre la protección de la vida privada, el respeto y la protección a la vida privada señalada en la Constitución solo se podía resguardar mediante el recurso de protección, y del cual, entre el año 1982 y el año 1997 no se verificaron más de cuarenta recursos de protección[55] tratándose de información comercial transmitida por DICOM S.A. Es más, podríamos señalar que en ese entonces (y nos aventuramos a aseverar que aún hoy) en el sector del mercado de la información la práctica habitual es la de la autorregulación de la información transable en el mercado.

[54] QUEZADA, Op. Cit., pág. 143.
[55] GUERRERO, Jaime. 1997. La empresa y la magistratura ante la acción de habeas data. Ius et Praxis, vol. 3, núm. 1. Universidad de Talca, Talca. Chile. pág. 217.

En ese entonces, el sector comercial tuvo una enorme reticencia en cuanto a la implementación del recurso del, habeas data, pues se temía que se produjera un término o restricción ilimitada para un sistema de información comercial que afectase la fe pública, que fuera un impedimento para la difusión de datos, noticias y mensajes provenientes de fuentes accesibles a público, el desaparecimiento del derecho a informar, la desnaturalización del derecho a informar y se información, y el término de la transparencia de la información[56]. Dicho sector fundamenta el mercado de datos pues en primer lugar las empresas del rubro de la información contribuyen a la democratización del crédito, a la mantención de tasas de interés en niveles aceptables lo que en definitiva se traducía en mayor acceso al crédito.

Sin embargo y pese al temor y reticencia que se tuvo en un principio, la experiencia ha demostrado que el Habeas Data no ha sido una herramienta eficaz y tampoco ha afectado al mercado de la información o acceso al crédito como se temió en su momento.

La deficiencia de la Ley N°19.628 se encuentra en que no se estableció un organismo de control independiente que tuviera la función de fiscalizar y sancionar. Asimismo, tampoco se estableció la obligación de registro de banco de datos privados la protección es en extremo débil.

Por otra parte, la normativa sería letra muerta si no existiera alguna acción judicial que tutelara el derecho a la vida privada, y los datos personales. En este sentido, y acorde a los principios rectores de la ley N°19.628 es que el habeas data constituye un cause procesal para resguardar los derechos y libertad de las personas en el ámbito de los datos personales, como por ejemplo, el derecho a la modificación, eliminación o bloqueo de datos personales. Consideremos además, que en nuestro país no existe una instancia administrativa ante la cual recurrir frente a la vulneración de estos derechos, por lo que el control de los mismos es a posteriori.

[56] GUERRERO, Op. Cit. Pág. 217 y 218.

El objeto del hábeas data 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[57]”. Su naturaleza jurídica es por tanto, una acción jurisdiccional que protege la libertad informática o el derecho de autodeterminación informativa. protección de la vida privada, la imagen, honra de las personas “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[58]”.

2.3.1 Bien jurídico protegido.

El bien jurídico protegido es el derecho a la autodeterminación informativa, el derecho a la protección de la vida privada o privacidad y la honra de la persona, igualdad ante la ley, la protección de la dignidad humana y la libertad, la veracidad y fidelidad de la información[59].

2.3.2 Sujeto activo y sujeto pasivo del habeas data

El sujeto activo del hábeas data es toda persona, nacional o extranjera, la que puede actuar personalmente o a través de su representante legal, según determinan las respectivas legislaciones[60]. por tanto, es el titular de los datos que ha visto vulnerado sus derechos.

El sujeto pasivo es el responsable del banco de datos, ya sea público o privado. De modo tal que la Ley N°19.628, en su artículo 14 señala que “Si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos”

---

[57] NOGUEIRA ALCALÁ, Humberto. Autodeterminación informativa y hábeas data en Chile e información comparativa. [en línea] <https://revistas-colaboracion.juridicas.unam.mx/index.php/anuario-derecho-constitucional/article/download/30267/27321> , pág 458. (Consulta: 30 de octubre de 2018)
[58] NOGUEIRA, Op. Cit. pág. 458.
[59] NOGUEIRA, Op. Cit. 466.
[60] NOGUEIRA, Op. Cit. 459.

2.3.3 Tribunal competente

El tribunal competente para conocer del hábeas data es el juez civil correspondiente al domicilio del responsable del banco de datos (domicilio del demandado), es decir, conforme a las reglas generales de acuerdo al artículo 134 del Código Orgánico de Tribunales.

2.3.4 Procedimiento

En nuestra legislación se contemplan tres tipos de procedimiento. El primero se trata de un procedimiento general de reclamo, el segundo se trata de un procedimiento especial de reclamo y el tercero será un procedimiento general.

2.3.4.1 Procedimiento general de reclamo:

La Ley N°19.628 se pone en dos hipótesis. En la primera hipótesis, y según el artículo 16 si el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o le denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, que se encuentre de turno según las reglas correspondiente, solicitando amparo.

El segundo caso dice relación con los artículos 17 y 18 de la Ley N°19.628 en el cual la acción debe ser presentada al juez y debe contener, por lo menos, una identificación clara de la infracción cometida por el responsable de la base de datos y los hechos en que se funda, acompañando los respectivos medios de prueba que lo acrediten.

En cuanto al procedimiento general, la acción debe ser notificada por cédula en el domicilio del banco de datos y el responsable del banco de datos deberá contestar traslado dentro quinto día hábil, indicando sus descargos y acompañando medios de prueba en que se funda. Si el demandado no tiene medios de prueba, debe indicarlo. Por el contrario, si ofrece prueba, el tribunal fijará audiencia para el quinto día hábil con el fin de recibir la prueba si es que no se ha acompañado.

Cabe señalar que esta facultad que se le entrega al demandado, facultad de la cual está desprovisto el titular de los datos personales, “constituye uno de los puntos más criticables de este procedimiento pues vulnera uno de los principios fundamentales de todo procedimiento cual es el de la bilateralidad de la audiencia, al dejar en manos del responsable del banco de datos, la posibilidad de que exista una audiencia de prueba, ya que si no ofrece prueba, no existirá tal audiencia[61]”.

Ahora bien, el tribunal puede adoptar las medidas que estime convenientes para hacer efectivos los derechos asegurados por la ley, conforme a lo establecido en el artículo 23 de la Ley N°19.628 “El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece”.

En cuanto a la valoración de la prueba, esta se apreciará en conciencia por el tribunal.

La sentencia definitiva se dictará dentro del tercer día luego de que ha vencido el plazo para presentar descargos (se hayan presentado descargos o no). Si se realizó audiencia de prueba, el plazo contará desde vencido el plazo fijado para rendir la prueba.

La sentencia definitiva se notificará por cédula y es apelable, en ambos efectos. Si se interpone recurso de apelación, se hará dentro de cinco días, término que es fatal. Dicho plazo se cuenta desde la notificación de la parte que lo entabla. Acorde a las reglas generales, la apelación debe contener los fundamentos de hecho y de derecho en que se funda y las peticiones concretas. Así, una vez deducida la apelación, se elevan los autos a la Corte de Apelaciones respectiva, la cual ordenará dar cuenta preferente al recurso, sin esperar la comparecencia de las partes. Sin perjuicio de lo anterior, la Corte puede ordenar traer los autos en relación y se oigan alegatos de los abogados de las partes, en cuyo caso se agregara a la tabla extraordinaria de la sala respectiva.

[61] JERVIS, Op. Cit. pág. 30.

El fallo que pronuncie la corte no es susceptible de casación, sin perjuicio de lo anterior, procede recurso de queja.

2.3.4.1 Procedimiento especial de reclamo.

Este procedimiento se utiliza en el evento de que el responsable de la base de datos se ha negado a entregar información argumentando razones de seguridad o interés nacional[62]. La reclamación será conocida por la Corte Suprema, la cual pedirá informa al responsable de la base de datos, debiendo ser expedita y fijándose plazo para la entrega de antecedentes. La Corte Suprema resolverá en cuenta.

Si se da el caso en que se reciba la causa a prueba, se abre un cuaderno separado, el cual será reservado. Asimismo, la Corte Suprema puede traer los autos en relación, en cuyo caso se oirán alegatos y la causa se verá en table extraordinaria. En este caso, la audiencia no es pública, sino secreta.

2.3.4.3 Procedimiento residual

Por último, en el caso de que no se contemple una acción dentro de los artículos 12 y 19 de la ley N°19.628, se aplica el procedimiento sumario, conforme a lo establecido en el artículo 23 de la misma ley.

Se aplica el procedimiento sumario en los casos en que el responsable del banco de datos no cumple con avisar a terceros que los datos han sido modificados o cancelados.

2.3.5 Sanciones.

Si el tribunal acoge la acción del reclamante, éste fijará un plazo prudencial para que el banco o registro de datos dé cumplimiento a lo ordenado. Asimismo, el tribunal puede sancionar con una multa que va desde 1 a 10 UTM, como determinar perjuicios si es que estos fueron solicitados.

[62] NOGUEIRA, Op.Cit, pág 468.

De no cumplirse lo anterior dentro del plazo ordenado por el tribunal, éste puede multar desde 2 a 50 UTM. Si se trata de un organismo público, el tribunal tiene la facultad de sancionar al jefe del servicio, con suspensión del cargo que va desde 5 a 15 días.

2.3.6 Responsabilidad.

En cuanto a la responsabilidad, el artículo 11 de la Ley N° 19.628 señala que “el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños”.

Por su parte, el artículo 23 de la misma ley, en su primer inciso, indica que “la persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular, o en su caso, lo ordenado por el tribunal.

De lo indicado en los artículos precedentes, podemos concluir que cuando la ley habla de debida diligencia, se entiende que el estándar exigido es la culpa o negligencia. es decir, no podemos hablar en este caso de que exista en estándar de responsabilidad estricta, de acuerdo a las reglas de responsabilidad del Código Civil.

2.3.7 Indemnización de perjuicios.

La indemnización de perjuicios será establecida prudencialmente por el tribunal, según la gravedad del caso en concreto y puede solicitarse mediante tres vías.

En primer lugar, puede solicitarse mediante el procedimiento del artículo 23 de la Ley N°19.628 en la cual se puede interponer la acción indemnizatoria en conjunto con la reclamación.

En segundo lugar, se puede solicitar en juicio sumario, cuando la infracciones de aquellas no contempladas en los artículos 16 a 19 de la Ley N° 19.628.

Por último, mediante una acción de indemnización de perjuicios en procedimiento ordinario, de acuerdo con las reglas generales del Código de Procedimiento Civil.

2.4 Acción de Protección

Una de las maneras en la que los titulares de datos han accionado ante los tribunales ordinarios es a través del llamado “recurso de protección” consagrado en el artículo 20 de la Constitución como una forma de resguardar los derechos que esta contiene en su artículo 19, argumentado que se ha infringido el derecho a la honra y vida privada consagrado en al artículo 19 en su numeral 4, estrategia utilizada por quienes han sentido vulnerados sus derechos con mucha anterioridad a la reciente consagración expresa del derecho a la protección de los datos personales en la ya comentada modificación constitucional del año 2018.

Dadas las particularidades de su procedimiento, esta acción se ha erigido como una forma rápida y efectiva de hacer frente a las vulneraciones de derechos de las personas en cuanto a sus datos, incluso antes de que la comentada modificación del texto del numeral 4 del Artículo 19 fuese discutida y en desmedro del procedimiento especial establecido por el Artículo 16 de la Ley de Protección de datos personales.

En este sentido es de gran relevancia en la materia el fallo Rol N°11.256-2011 de la Excelentísima Corte Suprema, el cual en su considerando Sexto dictaminó que: “cabe señalar que la existencia de un procedimiento especial contemplado en la Ley N°19.680 no obsta al ejercicio de la acción de protección, porque ésta puede ejercerse sin perjuicio de otros derechos”[63], refiriéndose a la procedencia de tal acción para obtener la eliminación de datos comerciales caducos del actor.

[63] Sentencia Rol N°11.256-2011 “Marchant Navarrete Fermin contra sr. Presidente de Banco Estado”. Corte Suprema, considerando sexto.

Es así que se ha asentado el criterio de que, de estimarse que se han vulnerado de forma ilegal o arbitraria los derechos del titular de los datos, éste podrá accionar ante las Cortes de Apelaciones sin necesidad de ejercer la acción especial de habeas data.

Lo anterior, sin embargo, no está exento de inconvenientes, por una parte, el ejercicio de la acción de protección no permite perseguir una eventual indemnización de perjuicios a favor del afectado y requiere que se estime que la conducta del recurrido sea calificada por la Corte de Apelaciones como ilegal o arbitraria.

Por otra parte, el recurso de protección es una acción de naturaleza individual, por lo que no permite accionar a favor de intereses colectivos o difusos, tal como quedó de manifiesto en la sentencia de la Excelentísima Corte Suprema de fecha 3 de junio de 2015, en causa Rol 5243-2015, la cual confirmó la sentencia de la Corte de Santiago rechazando el recurso de protección interpuesto contra la empresa 24x7 Limitada, desestimando que la publicación por el recurrido de los RUTS de las persona fuere un acto ilegal puesto que, en relación a los datos electorales revelados por el Servicio Electoral "habiéndose hecho públicos en internet por una institución del Estado los datos de las recurrentes con anterioridad a su tratamiento por el recurrido[64]", estos se encontraban contenidos en una "fuente accesible al público", además de estimar que con la sola publicación de sus datos en el rutificador se ha amenazado la vida privada de las recurrentes, y que además, en cuanto a los argumentos interpuestos por los recurrentes a favor de terceras personas, en particular menores de edad cuyos datos no pudieren haber sido obtenidos a través del Servicio Electoral, no puede acogerse el recurso ya que este no es una acción de carácter popular, limitándose su alcance únicamente a los recurrentes.

[64] Sentencia Rol N°5243-2015 "Zaror Miralles Danielle y otra contra Diaz Muller Sergio Andes". Corte Suprema, considerando séptimo.

Este fallo deja entonces en evidencia los siguientes obstáculos a los que se enfrenta la acción de protección para ser una alternativa procesal efectiva para la protección de los datos personales, pese a ser habitualmente utilizada para este fin:

- Es requisito acreditar que se está ante una conducta ilegal o arbitraria del recurrido
- Se debe acreditar que se ha amenazado uno de los derechos constitucionales amparados por esta acción
- Sólo puede ser interpuesta en favor de un interés particular, quedando afuera la posibilidad de accionar en pos de un interés “difuso”.

Dada la reciente modificación a nuestra Constitución es de esperar que el mal llamado recurso de protección siga siendo una de las estrategias favoritas de los titulares de datos cuya protección sea vulnerada, al encontrarse ahora expresamente consagrada su protección en el texto constitucional.

2.5 Acciones en la Ley de Protección al Consumidor

Otra fórmula que ha cobrado relevancia en el último tiempo consiste en proteger los datos personales a través de la invalidación judicial de cláusulas contractuales abusivas de acuerdo a lo dispuesto por la ley N° 19.496 Sobre Protección de los Derechos de los Consumidores. Se trata de una tendencia reciente, que tiene la particularidad de permitir proteger los intereses de personas indeterminadas a través de las competencias del Servicio Nacional del Consumidor.

En este sentido, resulta interesante revisar los siguientes fallos de nuestra Excelentísima Corte Suprema:

- Fallo de fecha 7 de julio de 2016 en causa N° 1.533-2015.

En este fallo, nuestra Corte Suprema se pronuncia sobre demanda colectiva por vulneración al interés difuso de los consumidores, en sede de casación en la forma y en el fondo, respecto a si corresponde declarar como abusivas y nulas las

cláusulas “Uso comercial” y “Política de privacidad de Ticketmaster”. En lo que nos atañe, esta última cláusula permitía a la empresa de venta de boletos para eventos Ticketmaster recolectar y revelar información de sus usuarios a terceros, por el solo hecho de utilizar el sitio web de la empresa para la compra de boletos, en términos amplísimos. La Corte anuló dicha cláusula bajo el argumento de que “resulta contraria a la buena fe, y en consecuencia abusiva, la obtención del consentimiento del titular de los datos mediante una condición general de contratación incluida en una transacción cuyo objeto principal es la entrada a un espectáculo. En el contexto de semejante transacción comercial, tal renuncia a la privacidad de los datos personales solo es válida si es otorgada en forma explícita y específica.[65]”

- Fallo de fecha 11 de octubre de 2016 en causa N° 4.903-2015

Esta sentencia se dicta en el contexto de un reclamo hecho por el Servicio Nacional del Consumidor en contra de la empresa Créditos Organización y Finanzas S.A. respecto del contrato denominado “Informativo Convenio”, el cual consideraban contenía cláusulas abusivas respecto a la información de los consumidores que habría sido divulgada.

En esta ocasión, la Corte Suprema, mantuvo el criterio asentado en el fallo precedente al considerar que el Servicio Nacional del Consumidor actúa dentro de su competencia al accionar en defensa del interés colectivo o difuso de los consumidores ante una cláusula de un contrato de adhesión que considere abusiva. A mayor abundamiento, la Corte, en el Considerando Décimo Tercero estableció que “si bien el tratamiento de datos personales está regulado en una ley especial, la afectación de intereses supraindividuales que implica la contratación en situación de desigualdad mediante contratos de adhesión cuyo contenido acarrea el desequilibrio entre las partes que se refleja, entre otros en el

[65] Sentencia Rol N°1.533-2015, “Servicio Nacional Del Consumidor Con Ticket Master Chile S.A.” Corte Suprema, considerando undécimo.

quebrantamiento de los derechos de los titulares de datos de carácter personal, constituye una materia susceptible de ser conocida en esta sede."[66]

- Fallo de fecha 6 de diciembre de 2016, en causa N° 26.932-2015.

Esta resolución se da en el contexto de un procedimiento por infracción a la Ley de Protección al Consumidor iniciado por el Servicio de Protección al Consumidor contra la empresa Ticketek Co. SpA., una compañía dedicada a la venta de boletos para espectáculos, por establecer, a su juicio, una serie de cláusulas abusivas en un contrato de adhesión que, entre las cuales que encuentran aquellas que autorizarían a la demandada en forma genérica a poner a disposición de otras empresas y para la utilización de servicios distintos al originalmente requerido por el titular de los datos, información de carácter personal, sin que haya tampoco constancia del derecho de los titulares de la información personal a revocar la autorización dada a la empresa. En esta oportunidad la Corte estimó que el tribunal de alzada estaba en lo correcto al considerar que el Servicio Nacional del Consumidor carecía de legitimación para accionar, puesto que "no es posible asumir que la ley especial pueda ceder ante la general, aun en el caso de procedimientos de interés colectivo o difuso de los consumidores, puesto que la naturaleza de los asuntos regulados por la ley 19.628 es esencialmente individual, sin que tengan cabida los procesos colectivos [67]"

Luego de este somero análisis, podemos entender que esta estrategia procesal igualmente enfrenta a lo menos, los siguientes obstáculos:

- Es necesario que estemos ante una relación de consumo cubierta por la Ley de Protección al Consumidor.

- Los tribunales y en particular la Corte Suprema no han sido consistentes en su criterio respecto a si es que el Servicio Nacional del Consumidor se encuentra

[66] Sentencia Rol N°4.903-2015 "Servicio Nacional Del Consumidor Con Créditos Organización Y Finanzas S.A". Corte Suprema.
[67] Sentencia Rol N°26.932-2015, "Servicio Nacional Del Consumidor Con Ticketek Co S.P.A." Corte Suprema, considerando sexto.

o no legitimado para accionar a nombre de los titulares de datos potencialmente afectados

A mayor abundamiento, debemos recordar que la Ley sobre Protección de los Derechos de los Consumidores también ha sido recientemente modificada durante el segundo semestre del año 2018, fortaleciendo las atribuciones del Servicio Nacional del Consumidor, por lo que debemos estar atentos al desarrollo que tales atribuciones puedan traer en la materia a medida que esta reforma entre en completa vigencia, tanto en sede administrativa como judicial. Resulta especialmente interesante la posibilidad de eventuales acciones colectivas en la materia, que permitan explorar la posibilidad de establecer procedimientos para los casos de vulneraciones masivas a los derechos de los titulares de los datos en su calidad de consumidores.

III. Conclusiones.

La era de la tecnología ha exigido una regulación legal y conceptual que sostiene y fundamenta la protección de datos personales, de modo tal que podemos encontrar en la Ley y la doctrina una serie de definiciones que comprende el concepto de protección de datos personales, sus elementos básicos y asimismo, una serie de principios y derechos que cumplen la función de completar el marco de protección de datos personales, y con ello poder dar una clasificación de los distintos tipos de datos personales.

De modo tal que se ha ido configurando un marco normativo a través del derecho comparado, en especial de Europa, y también un marco normativo en Chile que, a todas luces ha sido débil y poco efectivo en cuanto a la protección de los titulares de datos personales.

Finalmente, la ley ha dado procedimientos de protección de datos personales como la acción de protección y el habeas data, lo que se ha ido complementando a través de la jurisprudencia de tribunales ordinarios y el tribunal constitucional.

Capítulo III: EL MERCADO DE DATOS PERSONALES Y SU REGULACIÓN

I. Tratamiento por organismos públicos y privados

Tanto los organismos públicos como privados realizan constantemente tratamiento y transferencia de datos personales. Por cierto, las finalidades con las que se lleva a cabo el tratamiento de datos personales es distinto, aunque comparten más o menos el mismo normativo (a grandes rasgos la Ley de Protección de la vida privada y la Constitución Política), con todo, en los ámbitos público y privado se aplica con más o menos intensidad cada uno de los principios y obligaciones que prescriben las leyes y la constitución.

1. Tratamiento por parte de Organismo Públicos.

Con el fin de transparentar los actos de la administración del Estado, se realizaron varios intentos de dotar de transparencia la actividad de los organismos públicos. Con la publicación de la ley N°20.285 sobre Transparencia y Acceso a la Información pública se logró finalmente dicho propósito, lo que significó que los ciudadanos ya no tenían que ceñirse a reglas propias de cada institución o quedar a merced de la discrecionalidad de cada organismo sino que ahora se tendría un procedimiento para el ejercicio y amparo del derecho de acceso a la información pública.

Dicho esto, tanto la Ley de Transparencia como la Ley de Datos personales establecen el marco normativo que rige el tratamiento de datos aplicable al sector público.

La Ley N°20.285 Sobre Acceso a la Información Pública o también llamada Ley de Transparencia estableció a través del Consejo para la Transparencia la obligación de velar por la Ley N°19.628 o Ley de Protección de la Vida Privada en la gestión de los organismos públicos.

Así, todos los servicios públicos y órganos de la administración del Estado requieren tratar datos, administrándolos de diversas formas, en su mayoría computacional. Por ejemplo, para poder acceder al patrocinio de un abogado de

la Corporación de Asistencia Judicial, se debe obtener previamente el Registro Social de Hogares (antigua ficha de protección social), el cual requiere nombres completos de un grupo familiar, domicilios, renta, deuda, gastos básicos del hogar etc., o para poder tomar decisiones trascendentales para el país, como fijar políticas públicas.

De modo tal que el Estado se transforma en el mayor tenedor de datos personales. Consecuente con ello "Al derecho público le corresponde establecer <límites> y <restricciones>. Los primeros, para que no se vulnere la intimidad de las personas cuyos datos se procesa. Las segundas, para que sólo se usen los datos personales dentro de la competencia exclusiva de los servicios públicos y para sus fines específicos[68]" y siempre teniendo en cuenta el cumplimiento de sus fines.

El marco regulatorio respecto de la administración del Estado es amplio, ya que existen leyes generales y especiales, reglamentos y dictámenes de organismos fiscalizadores cuyo fin es determinar parámetros constitucionales y administrativos para el tratamiento de datos personales, teniendo como horizonte los fines promocionales y asistenciales del Estado.

Cabe destacar que es la propia Ley de Datos Personales, en su artículo 20, la que faculta a todo organismo público a efectuar cualquier tratamiento de datos personales, sin autorización del titular, dentro de la órbita de su competencia, para lo cual no se requiere de texto específico que autorice el tratamiento de datos personales; sólo se necesita que este se inserte dentro de la esfera de sus atribuciones y competencias que tiene asignada por ley[69].

Asimismo, la ley exige que las instituciones estén en el Registro de Banco de Datos a cargo del Registro Civil e Identificación. Sin embargo, el no cumplimiento

[68] JIJENA LEIVA, Renato. 2003. Tratamiento de datos personales en el Estado y acceso a la información pública. Revista Chilena de Derecho y Tecnología. Centro de estudios de derecho informático. Universidad de Chile Vol. 2 Núm. 2, pág. 52.
[69] MATUS ARENAS, Jessica. 2013. Derecho de acceso a la información pública y protección de datos personales. Revista Chilena de derecho y tecnología. Centro de estudios de derecho informático. Universidad de Chile, ISSNN 0719-2576. Vol. 2 NÚM 1, pág. 199.

de la obligación de registrarse no tiene sanción y hasta la fecha no todas las instituciones han cumplido.

Al respecto, el Consejo Para La Transparencia, se le ha otorgado al atribución de velar por el cumplimiento de la Ley de Datos Personales, ha dado algunas recomendaciones, por ejemplo las “Recomendaciones del consejo para la transparencia sobre protección de datos personales por parte de los órganos de la administración del estado” de fecha 5 de septiembre del año 2011, que señaló como unos de sus objetivos elevar los estándares de protección de datos personales, dado los casos de acceso ilegales a registros administrados por órgano del Estado respecto de datos personales.

En dichas recomendaciones se hace una definición de los conceptos fundamentales que otorga la Ley de Protección de Datos Personales, los principios orientadores de los mismos, derechos de los titulares, obligaciones específicas de los organismos del Estado, su tratamiento y medidas de seguridad.

En este ámbito, y como se dijo antes, el Estado es el mayor tenedor de bases de datos, y en los casos en que dichas bases de datos de los organismos del Estado no son fuentes públicas de información, la Administración solo puede permitir el acceso su acceso a los datos personales:

1) A los servicios públicos, a los tribunales y a las entidades facultadas por ley
2) a los propios titulares y propietarios de los antecedentes[70]

Así, para evaluar si procede o no la entrega de información, la administración debe considerar:

1) la naturaleza concreta de los requirentes
2) la naturaleza de la información solicitada (pública, privada, secreta o reservada, nominativa o disociada, relacionada etc.)

[70] JIJENA, Op. Cit. pág. 55.

3) Si existe - o no- una obligación expresa establecida por ley para proceder a la entrega de la información

4) <la finalidad de los requerimientos de datos o información personal>[71]

Siguiendo a JIJENA, a nivel jurídico, la evaluación para proceder a entregar información personal nominativa debe considerar, primero, "estudiar la procedencia o no teniendo presente lo que establezcan normas generales de derecho público, como la Ley de Bases de la Administración del Estado" en segundo lugar, habla de considerar lo que digan las leyes especiales o relacionadas con la naturaleza específica de la gestión del servicio público[72]. Y por último lo que dispongan las leyes especiales como la Ley Sobre Protección de la vida privada N°19.628 y la Ley de Transparencia N°20.285.

Con ello se puede determinar la naturaleza de los datos, si el servicio público es competente y la naturaleza de la entidad que solicita dicha información y por supuesto los fines con los que lo hace.

Por otra parte, cabe señalar el derecho de petición de todos los ciudadanos, que la Constitución y la Ley de Bases Generales de la Administración ha otorgado para tal efecto. los cuales se pueden ejercer ante Tribunales o ante la Contraloría. ¨Por ello, al ser el Estado responsable de la base de datos que procesa y almacena, los servicios públicos deben dar cumplimiento a sus deberes establecidos por ley.

Cabe señalar además, que las normas que regulan el procesamiento de datos personales sobre los ciudadanos, son leyes permiten que los datos personales sean tratados sin el consentimiento expreso previo del titular (la regla general es que siempre exista este consentimiento, pero las excepciones son tan amplias que en el fondo, invierte la regla).

Por eso "determinar los criterios jurídicos aplicables, los deberes, las limitaciones y las responsabilidades de los funcionarios públicos, por un lado, y los derechos

[71] JIJENA, Op. Cit. pág. 55 y 56.
[72] Ibid.

de los ciudadanos, por el otro, no se logra sólo con el análisis del articulado de la ley 19.628”

Ahora bien, dentro de las obligaciones que tienen los organismos públicos en materia de protección de datos, estos deben cumplir con los principios de información de calidad de los datos y seguridad de los mismos, como también, la inscripción de sus bases de datos en el Registro Civil.

El Consejo, a través de sus decisiones ha señalado la reserva de información cuando contiene datos personales. Con todo, el Consejo aplica lo que se conoce como test de daños e interés público.

El test de daños (o también principio de proporcionalidad) “consiste en el balance entre el interés de retener la información y el interés de divulgarla para determinar si el beneficio público resultante de conocer la información solicitada es mayor que el daño que podría causar su revelación; en el presente caso de proteger la vida privada de una persona determinada[73].”

En concreto, se pretende analizar 1) si la medida es eficaz 2) si no existe un medio más moderado para la consecución eficaz del propósito buscado y 3) si de la medida a adoptar, derivan más beneficios que perjuicios sobre otros bienes o valores en conflicto[74].

2. Tratamiento por parte de entidades privadas.

Hoy en día no es difícil adivinar y constatar que nuestros datos personales son manejados por diversas instituciones, tales como bancos, farmacias, compañías de seguros, tiendas de retail, clínicas, administradoras de fondos de pensiones, supermercados, redes sociales, hasta conocidas tiendas de cafés de las grandes ciudades, de modo tal que todas las transacciones que realizamos día a día están en manos de instituciones privadas que manipular y cruzan dicha información, sin

[73] MATUS, Op. Cit. pág. 208.
[74] Ibíd.

que seamos consciente de ellos o si quiera se nos haya solicitado autorización para su tratamiento.

A cada momento esta información conforma volúmenes inimaginables de datos en alguna base de datos, a lo cual las leyes actuales no han llegado a regular del todo bien, es más, ni siquiera se ha llegado a un estándar aceptable en la materia. Al respecto, en un artículo publicado el 23 de julio del año 2015[75] la OCDE advierte a Chile por el retraso en materia de protección de datos personales.

Así por ejemplo, en materia de tratamiento de datos personales en internet, se ha desarrollado todo un servicio de industrias de Tecnologías de la Información y Comunicación, que ha convertido a los datos en activos para las empresas y productos de valor económico relevante.

En muchos casos no tenemos conocimiento de que se está generando información sobre nosotros, ni quien la controla. Así, el Foro Económico Mundial considera que efectivamente, la información es una nueva clase de activos[76]. Es tal el volumen de información, que hoy en día también se habla de lo que se conoce como Big Data, cuando estamos ante datos masivos de información.

En cuanto al tratamiento de datos en la tecnología, se siguen tres consecuencias importantes: Primero, cada vez que los datos dependen de la tecnología, la propiedad de los mismo queda en manos del titular de dicha tecnología, por ejemplo, cuando se hace una compra a través de una tarjeta de crédito en alguna tienda. En segundo lugar, la estructura, la representación, el almacenamiento y la aplicabilidad potencial de los datos depende de la naturaleza de cómo se recogen los datos, afecta la forma en que se pueden utilizar[77].y en tercer lugar, la

[75] ALONSO, Carlos. 2015. OCDE envía carta de advertencia a Chile por retraso en protección de datos personales. [en línea] <http://www.pulso.cl/economia-dinero/ocde-envia-carta-de-advertencia-a-chile-por-retraso-en-proteccion-de-datos-personales/> (Consulta 01 de octubre de 2018).
[76] ANAHIBY BECERRIL, Gil. 2016. Personally Identifiable Information, Big Data y Personal Data Store Personally Identifiable Information, Big Data and Personal Data Store. Revista Iberoamericana De Derecho Informático (Segunda Época). Federación Iberoamericana De Asociaciones De Derecho E Informática. Año 1, N°1, pág. 31.
[77] ANAHIBY, Op. Cit. pág. 32.

privacidad y confidencialidad y seguridad de los datos, pueden tener graves problemas, ya que su utilización puede afectar comportamiento individual de las personas. Asimismo, cada vez que se generan datos personales, la eliminación de los mismos es imposible.

Esto ha generado que exista una asimetría entre las instituciones que manejan información y los individuos (titulares de los datos)

II. La información como bien económico

Para nadie es un misterio que la información es valiosa. Pensando en términos económicos, entre más y mejor información tengamos sobre un determinado asunto, mejores decisiones seremos capaces de tomar, maximizando nuestro beneficio. Es por ello es que la teoría económica considera a la información que tengan los agentes de un determinado mercado una variable de suma importancia para el funcionamiento del mismo, ya que disrupciones en el flujo de ésta dan origen a “fallas de mercado”.

Pero la información no es solo una variable a considerar a la hora de analizar cualquier mercado en cual se transe un determinado bien, si no que se trata de un bien en sí misma, que puede ser objeto de transacciones, con un valor propio y que posee una serie de características que lo distinguen de otras clases de bienes. De hecho, es posible pensar en un “mercado de la información”, con sus agentes, características e incluso fallas particulares.

Sin ahondar demasiado en las definiciones que ha dado la doctrina sobre ella, podemos entender que la información es el conocimiento que surge una vez que una serie de datos han sido organizados, para los efectos de este trabajo utilizaremos la conceptualización de JERVIS quien entiende a la información como “cualquier antecedente o dato que pueda ser utilizado por los agentes de la

economía para generar conocimiento"[78], así es como los datos se transforman en información una vez que son interpretados y dotados de significado[79].

En cuanto a las características particulares que tiene la información como un bien económico podemos decir que a) la misma información puede ser utilizada de distintas maneras, por distintos agentes y con distintos propósitos e intereses sin que esta se "agote" o "destruya" por el uso dado, b) aquello puede suceder simultáneamente, prácticamente sin limitaciones, c) ella tiene la capacidad de generar nuevos "productos", y d) los usos adicionales de la información ya obtenida tienen un costo relativamente bajo.

Finalmente es bueno recordar que la información es un bien que es objeto de derechos de propiedad y relaciones contractuales, como por ejemplo en el caso de los "acuerdos de confidencialidad", o de los secretos industriales, en los cuales se protege cierta información considerada valiosa de ser divulgada, especialmente para evitar que caiga en manos de competidores.

1. El mercado de la información

Aprovechando estas características particulares, la información de toda clase, desde siempre, se ha "entregado" de un agente a otro generándose un verdadero mercado, con miles de actores y millones de transacciones cuyo valor es, en conjunto, incalculable. La información transada puede ser sobre cualquier ámbito de la vida, provenir de las más diversas fuentes, con la consecuente diferencia en su calidad, y venderse a los más disímiles precios.

[78] JERVIS, Op. Cit. pág.22.
[79] Para mayor información, véase NIMMER Raymond y KRAUTHAUS Patricia, Information as a Commodity: New Imperatives of Commercial Law. [en línea] Law and Contemporary Problems Vol. 55, Summer 1992 < https://scholarship.law.duke.edu/lcp/vol55/iss3/4/> (Consulta 20 de noviembre de 2018).

Es tal la importancia de este “mercado de la información” que existen compañías dedicadas completamente a obtener, procesar y vender información, participando también los gobiernos e instituciones públicas.[80]

2. El mercado de la información personal

Sin embargo, particular importancia reviste este mercado cuando el bien transado son los datos personales de otros, no solo por las implicancias económicas ello, sino que también por los aspectos sociales y jurídicos en juego.

Como sabemos, la información que es transada en este “mercado de la información” puede ser sobre la más amplia variedad de asuntos, sin embargo, dadas sus implicancias económicas, sociales y jurídicas nos concentraremos en las transacciones de “información personal”, es decir aquella trata sobre las personas.

La información personal no solo es transada en el mercado general de la información, sino que es parte de un submercado de la información sumamente lucrativo, moviendo cantidades impresionantes de dinero a lo largo y ancho del planeta, y que todo indica seguirá dicha tendencia en el futuro, pero, debido a que precisamente lo que se encuentra en juego son datos personales de individuos, es evidente que no basta observar este fenómeno desde una perspectiva económica, sino que se debe poner especial atención a los derechos de las personas cuya información se encuentra circulando.

Tal como comentábamos en el acápite anterior, existen entidades, tanto públicas como privadas, dedicadas a las transacciones de información, pues bien, especial relevancia tienen aquellas que se dedican a obtener, procesar y vender información sobre las personas, la cual es adquirida por los más diversos agentes, para infinidad de usos, destacando “los gobiernos, las instituciones de crédito, las

[80] Para mayor información, véase NIMMER Raymond y KRAUTHAUS Patricia, Information as a Commodity: New Imperatives of Commercial Law. [en línea] Law and Contemporary Problems Vol. 55, Summer 1992 <https://scholarship.law.duke.edu/lcp/vol55/iss3/4/> (Consulta: 20 de noviembre de 2018).

compañías de seguros, las agencias de reportes de crédito son los mayores compradores de información personal."[81]

Dadas las particularidades de este mercado, hace ya décadas que se tiene conciencia de la necesidad de regularlo, a través de diferentes mecanismos tal como vimos en la primera parte de este trabajo.

III. El mercado de datos personales

1. Caracterización del mercado de datos personales

Es importante destacar que, en nuestro país, como prácticamente en todo el mundo, el tratamiento de datos personales con fines lucrativos es una actividad económica absolutamente lícita, sin perjuicio de ser susceptible de ser regulada y limitada, tal como vimos al analizar la Ley de Protección de la Vida Privada, la cual, pese a su precariedad reconoce la importancia y la necesidad de armonizar los intereses y derechos de, por una parte, los titulares de los datos, y por otra, de quienes deseen tener acceso a ellos.

En cuanto a las características del mercado nacional, vemos que este sigue la tendencia mundial de expandirse con rapidez tanto en el volumen de datos recopilados como en naturaleza de los mismos. También observamos que existen diversos actores que participan de él, para ello utilizaremos la clasificación hecha por JERVIS[82], la cual consideramos continúa siendo acertada para la descripción de este, según esta autora, es posible distinguir como elementos del mismo:

a) fuentes primarias de información personal, esto es, las personas o entidades que

entregan al mercado en forma directa datos personales.

[81] LAUDON, Kenneth, Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information. [en línea]. NYU Working Paper No. IS-97-04, enero 1997 < https://ssrn.com/abstract=1283008 > (Consulta: 20 de noviembre de 2018).
[82] JERVIS, Op.Cit., pág.161.

b) fuentes secundarias de información personal, esto es, aquellos que distribuyen la referida información, comunicándola a terceros, generalmente en forma onerosa, y

c) usuarios finales de datos personales, son aquellos que buscan y adquieren la información personal para uso propio y que pueden ser personas naturales o jurídicas.

Jervis además hace presente que por expresa disposición del inciso final de la Ley 19.628, quedan excluidos de este mercado las personas jurídicas privadas que tratan datos personales para el beneficio propio de ellas o de sus afiliados, al no poder divulgar sus datos.

1.1 Mercado de datos patrimoniales

Es posible sostener que, en Chile, uno de los aspectos del mercado de datos personales que mayor atención ha obtenido tanto por los legisladores, académicos y agentes del mercado son los datos patrimoniales de los individuos, lo que ha dado origen a regulaciones especiales respecto a los mismos. Estos datos se refieren tanto a los aspectos positivos como negativos de la situación económica de una persona y abarcan elementos tales como su historial crediticio, estados financieros y morosidades, entre otros.

Es fácil apreciar que esta información resulta especialmente valiosa para las instituciones financieras, pues permite generar modelos de riesgo crediticio, establecer tasas de interés, y finalmente influenciar la decisión de si contratar o no con un individuo.

Tan relevante resulta esta información que en los últimos años incluso ha servido de base para la toma de decisiones que en una primera instancia podrían resultar ajenas al ámbito financiero, tales como suscribir contratos de arrendamiento o incluso contratar a alguien para un puesto de trabajo.

Contrario a lo que intuitivamente uno pudiera pensar, la difusión de los datos patrimoniales de un particular es una de las áreas que mayor pie da para la

vulneración de los derechos de los mismos, es por eso que se han desarrollado una serie de iniciativas para transparentar la información que existe en las bases de datos y facilitar su control por parte del titular de la misma, siendo probablemente el caso más icónico la ley Ley N°20.575, conocida como "No más DICOM".

1.2 Mercado de datos de identificación

En este caso, los datos transados son precisamente aquellos que sirven para singularizar a una persona como tal, como su nombre, RUN o huella dactilar, entre otros.

En Chile, el principal agente en cuanto a bases de datos de identificación es el Estado, particularmente a través del Servicio de Registro Civil e Identificación, el cual no solo organiza y guarda dicha información, sino que también la distribuye a otras entidades públicas y privadas, estas últimas a cambio de una contraprestación económica, las cuales las utilizan a su vez para los más diversos fines, los cuales pueden ir desde servicios de cruce de información, como los llamados "rutificadores", como la prestación de servicios de seguridad, por dar solo un par de ejemplos.

Pero no solo el Estado actúa recopilando esta clase de datos, en los últimos años ha habido un creciente interés por parte de las entidades privadas por hacerse de esta valiosa información, ya sea para su propio uso o venta a terceros. En dicha misión uno de los datos más codiciados es el RUN o Rol Único Nacional, el cual es un dígito irrepetible otorgado a cada chileno o bien extranjero residente en Chile por el Servicio de Registro Civil e Identificación, el cual hace las veces de identificador universal dentro del territorio nacional, lo cual claramente abre la puerta a toda clase de cruces de información para ampliar las bases de datos de estas compañías respecto a sus usuarios, generalmente con la intención de generar perfiles de los mismos para fines de marketing.

Lo anterior ha llevado a las más imaginativas prácticas para lograr que los titulares de datos entreguen voluntariamente y gratuitamente tal dato, desde condicionar

la aplicación de ofertas, regalos o concursos a su entrega hasta derechamente negarse a prestar un servicio o vender un producto si es que la persona no accede a ello.

Como podemos observar en el caso de los datos de identificación los agentes que en mayor medida aportan los mismos al mercado son el Estado y los propios titulares. Por otra parte, el mayor valor de estos datos corresponde a la posibilidad que brindan de ser cruzados con otros respecto de un mismo individuo para generar perfiles más completos del mismo.

1.3 Mercado de datos personales en internet

En esa categoría lo relevante no es la clase de dato personal tratada, sino que el "lugar" en donde ello ocurre: el Internet. El tratamiento de los datos recabados en la internet puede responder a los más variados fines y no conoce de fronteras geográficas.

Hoy en día prácticamente todos utilizamos la red en mayor o menor medida y entregamos a ella nuestros datos personales, ya sea en forma consciente, (teniendo, en todo caso, el titular de los datos muy variables grados de comprensión respecto al tratamiento que se le dará a su información, e incidencia sobre ello) como cuando creamos un perfil para participar en una red social o inconsciente a medida que hacemos uso de los distintos sitios y aplicaciones que nos ofrece la web a través del llamado "tratamiento invisible de datos personales" el cual "consiste en un conjunto de operaciones y procedimientos técnicos efectuados por programas y equipos capaces de procesar los datos de los usuarios y ponerlos a disposición de terceros sin conocimiento o consentimiento de sus titulares."[83]

[83] HERRERA BRAVO, Rodolfo. Privacidad e Internet: El problema del tratamiento invisible y automatizado de datos personales, Derecho Público Contemporáneo. Agrupación Nacional de Abogados de la Contraloría General de la República, v.2, no.5:, 2001, May./Ago., pág .58.

Dentro de la información recolectada se encuentra, por ejemplo, la dirección IP[84], direcciones de correo electrónico, números de teléfono móvil, sistema operativo y navegador utilizados, historiales de búsquedas y de navegación y geolocalización, datos que como podemos apreciar, han nacido a partir precisamente de la creación del internet y que pueden en ciertos casos ser calificados como personales. Todo lo anterior permite configurar un verdadero perfil del usuario que se encuentra navegando.

Una las principales de las finalidades para esta recolección de datos es el perfilamiento de los usuarios, específicamente para fines de marketing y publicidad[85]. A través de los cruces de información es posible generar un perfil de un determinado usuario y así ofrecerle productos y servicios que calcen con sus intereses. En este contexto existen dos clases de publicidad particularmente eficientes y de gran interés para los oferentes, a saber, la publicidad contextual y el remarketing. La publicidad contextual hace alusión a la colocación de anuncios en un sitio web, los cuales han sido automáticamente seleccionados de acuerdo al contenido de la página, a través de plataformas como Google AdSense, por otra parte el remarketing consiste en mostrar anuncios referentes a productos que el usuario ya ha visto navegando por la red. Ambas clases de publicidad son del tipo "conductual" ya que implican el monitoreo de la actividad un usuario basada en su dirección IP.

Una de las principales herramientas informáticas para la recolección de información personal de los usuarios de internet son las cookies, las cuales "son un conjunto de caracteres que se almacenan en el disco duro o en la memoria temporal del computador de un usuario cuando accede a las páginas de

[84] La Sentencia del Tribunal de Justicia de la Unión Europea de 19 de octubre de 2016 (Patrick Beyer v. Bundesrepublik Deutschland), señaló que "una dirección IP dinámica registrada por un proveedor de servicios de medios en línea con ocasión de la consulta por una persona de un sitio de Internet que ese proveedor hace accesible al público constituye respecto a dicho proveedor un dato personal, en el sentido de la citada disposición, cuando éste disponga de medios legales que le permitan identificar a la persona interesada gracias a la información adicional de que dispone el proveedor de acceso a Internet de dicha persona".

[85] ESTEVE, Asunción, The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. [en línea] International Data Privacy Law, Vol. 7, issue 1. <https://doi.org/10.1093/idpl/ipw026> (Consulta: 6 de enero de 2019).

determinados sitios web."[86] y que permiten determinar el perfil de navegación de un usuario. Existen dos grandes categorías de cookies: las de sesión, las cuales se recogen únicamente durante la estadía del usuario en el sitio web, y las persistentes, las cuales se quedarán almacenadas por mayor tiempo[87].

Si bien las cookies son una herramienta ampliamente utilizada para la recolección de datos de los usuarios de internet, ciertamente no son la única, y con el avance de la tecnología es de esperar que cada día estas herramientas sean más sofisticadas, sobre todo si tenemos en cuenta la creciente regulación a la que se ven sometidas, tales como el Reglamento General de Protección de Datos Personales de la Unión Europea, el cual en su Art. 30° señala que las cookies pueden ser consideradas datos personales cuando permiten la identificación de un individuo, por lo que les resultaría aplicable dicha normativa.

Otra clase de herramienta, similar a las cookies, son los llamados "pixeles de seguimiento", los cuales son un gráfico diminuto, camuflado dentro de un sitio web, el cual al ser visitado ser visitado será procesado por el navegador del usuario y permitirá al operador del "pixel" conocer datos tales como el navegador utilizado, la hora de conexión, actividad en el sitio web la dirección IP del usuario. También existen softwares maliciosos, como los spyware que se instalan furtivamente en un dispositivo a fin de recolectar información del mismo para ser enviada a un tercero, y adwares, los cuales actúan en forma similar, pero su fin es enviar publicidad al usuario.

La información de los usuarios de la web, resulta extremadamente valiosa, al punto que hoy en día los gigantes de la web, como por ejemplo Google y Facebook sustentan su modelo de negocios en la venta y colocación de publicidad a la medida del perfil de cada usuario y existen numerosos "data brokers" dedicados

[86] DICCIONARIO DE TÉRMINOS INFORMÁTICOS [en línea] <http://www.moheweb.galeon.com/diccinformatic.htm#C>, (Consulta: 05 de marzo de 2019).
[87] Véase. COFONE, Ignacio; The way the cookie crumbles: online tracking meets behavioural economics. [en línea] International Journal of Law and Information Technology, Vol. 25, issue 1, <https://doi.org/10.1093/ijlit/eaw013> (Consulta: 25 de noviembre de 2018).

a transar dicha información, algunos de los cuales son verdaderos gigantes corporativos como en el caso de las compañías Acxiom, Oracle, Datalogix, PeekYou y Recorded Future, entre muchas otras. Esto sumado al inevitable crecimiento de la web y sus aplicaciones solo permite prever que los volúmenes de información personal tratadas a partir de ella sólo podrán aumentar en el futuro, abriendo camino para más y más complejos usos de la misma.

1.4 Mercado de datos de salud y médicos

En esta categoría de datos encontramos aquellos referentes a los medicamentos recetados y comprados por las personas, por lo que pueden ser considerados además como datos sensibles. En este caso uno de los principales agentes recopiladores de datos son las farmacias, quienes llevan registros de las compras que hacen los pacientes.

Posteriormente esta información es vendida a laboratorios farmacéuticos, empresas de seguros e ISAPRES. Existen además otros interesados en adquirir esta información, tales como las agencias de crédito, quienes pueden a través de estos datos generar perfiles de riesgo de sus potenciales clientes.

En cuanto a las estrategias utilizadas para recopilar la información, esta por lo general es entregada voluntariamente por sus titulares, a través de estrategias como las vistas en el apartado sobre datos de identificación, lo cual permite la confección de bases de datos de mayor calidad y valor comercial.

1.5 Mercado de datos personales para fines de marketing o publicidad

Buena parte de los datos personales que son tratados lo son con fines publicitarios o de marketing directo, es decir, se hace uso de los mismos para persuadir a un posible consumidor de adquirir un determinado bien o servicio.

Lo anterior puede hacerse de las más variadas, e increíbles por lo demás, formas, desde algo tan simple como contar con una base de datos en soporte físico que contenga una serie de direcciones postales en donde enviar folletos publicitarios, hasta las sofisticadas técnicas de perfilamiento de usuarios de una red social. Por

otra parte, quien realiza el tratamiento puede hacerlo por su cuenta, para la venta de sus productos o servicios, o bien puede contratar para ello a alguna de las miles de empresas especializadas que existen en todo el mundo.

En cuanto a los datos personales específicos utilizados para fines publicitarios, suelen ser aquellos que permiten la identificación y localización de una persona, a fin de poder hacerle llegar el material promocional, sin embargo, cualquier dato personal puede eventualmente ser utilizado con fines de marketing, como resultado de proceso de perfilamiento[88].

Respecto a las fuentes de donde se obtienen los datos, éstas también son de las más variadas, yendo, por ejemplo, desde la entrega voluntaria de los mismos por parte de sus titulares, pasando por la compra de bases de datos que otras empresas hayan obtenido hasta llegar a las más sofisticadas técnicas de espionaje cibernético o incluso, el robo de información.

Dado el crecimiento que ha tenido esta industria y la agresividad de las técnicas empleadas es que ha surgido una preocupación respecto a los límites que se deben aplicar en pos de asegurar los derechos de los titulares de los datos, sin perjuicio de ello debemos recordar que de acuerdo a la Ley Sobre Protección a la Vida Privada no se requiere el consentimiento para el tratamiento de los datos cuando sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Un caso paradigmático de nuestro país fue la creación por parte del Servicio Nacional del Consumidor de la aplicación "No molestar"[89] a fin de poner un freno al acoso que sufren millones de personas y que facilita, al menos en teoría, la eliminación del número de teléfono, dirección postal y correo electrónico del solicitante que ha manifestado su deseo de no recibir comunicaciones por parte del proveedor de los servicios, de sus registros, bajo el alero del art. 28 b de la Ley 19.496 Sobre Protección de los Derechos de los Consumidores. "Toda

[88] JERVIS, Op. Cit., pág. 171.
[89] Servicio Nacional del Consumidor. [en línea] <https://www.sernac.cl/app/no-molestar/> (Consulta: 15 de diciembre de 2018).

comunicación promocional o publicitaria enviada por correo electrónico deberá indicar la materia o asunto sobre el que versa, la identidad del remitente y contener una dirección válida a la que el destinatario pueda solicitar la suspensión de los envíos, que quedarán desde entonces prohibidos.

Los proveedores que dirijan comunicaciones promocionales o publicitarias a los consumidores por medio de correo postal, fax, llamados o servicios de mensajería telefónicos, deberán indicar una forma expedita en que los destinatarios podrán solicitar la suspensión de las mismas. Solicitada ésta, el envío de nuevas comunicaciones quedará prohibido“[90].

Finalmente, ya que hoy en día gran parte de los datos que se tratan en Internet son utilizados para fines de mercadotecnia, generando una industria millonaria, es que retomaremos algunos aspectos de esta categoría cuando nos explayaremos con mayor detalle respecto al tratamiento de datos personales en Internet

1.6 Mercado de datos personales públicos

En este caso se trata de los datos personales manejados por el Estado, como hemos visto con anterioridad diversos órganos del mismo manejan información sobre las personas, la cual comparten no sólo con otras reparticiones públicas, sino que eventualmente y si es que se encuentran facultados para ello, también con entidades privadas, o bien directamente con particulares. Por mencionar algunos órganos públicos que manejan gran cantidad de datos personales tenemos el caso del Servicio de Registro Civil e Identificación, el Servicio Electoral y el Servicio de Impuestos Internos. Dentro de las particularidades de estos datos podemos mencionar que estos tienen su origen precisamente en un acto de la administración, como lo es el otorgamiento de un RUN o bien que resulta obligatorio para los particulares entregar la información al servicio que lo solicite, el cual puede a su vez compartirla con otros órganos públicos. A modo de ejemplo podemos decir que el Servicio de Registro Civil e Identificación es el encargado de inscribir el nacimiento de un nuevo chileno, momento en el cual le asignará un

[90] Art. 28 b de la Ley 19.496 Sobre Protección de los Derechos de los Consumidores.

RUN. Posteriormente cualquier persona que conozca dicho dígito podrá adquirir de este Servicio un Certificado de Nacimiento, el cual a su vez contendrá información sobre el nombre, RUN, fecha de nacimiento, identidad de los padres y localidad de inscripción de la persona a cual éste designe.

Especial atención merecen los datos contenidos en el padrón electoral, puesto que hoy se considera como información pública gracias a una interpretación dada por el Consejo para la Transparencia, y hasta el año 2010 el SERVEL lo tenía publicado para la venta en su catálogo, al precio de lista de $21.698.799. En él se encuentra información referente a todos los chilenos mayores de 18 años, considerándose como datos personales públicos: a) sus nombres y apellidos, b) números de Rol Único Nacional, c) sexo, d) domicilio electoral y e) número de mesa en el que les corresponde votar.

Por otra parte es importante señalar que el art. 4° del DFL N°5 prohíbe el uso del padrón para fines comerciales, lo cual se ve reforzado con sanciones penales.

De igual manera, si es que el Servicio Electoral hace entrega del padrón debe cumplir con lo exigido por el Art. 5 de la Ley 19.628, en cuanto a indicar a) la individualización del requirente; b) el motivo y propósito del requerimiento, y c) el tipo de datos entregados, sin embargo el "SERVEL no fiscaliza los segundos usos de la información[91]". Sin perjuicio de lo anterior, debida a la amplia difusión que ha tenido el padrón electoral para la elaboración de bases de datos, es fácil intuir que la información en él contenida hoy forma parte del mercado para distintos fines, incluida la propaganda política y marketing.

[91] GARRIDO, Romina. 2018. Datos personales e influencia política en Chile". Informe realizado por Derechos Digitales [en línea] https://datosprotegidos.org/wp-content/uploads/2018/09/Informe-datos-electorales.pdf, pág. 25(Consulta: 4 de diciembre de 2018).

IV Regulación del mercado de datos personales

1. Introducción

Como hemos podido apreciar, tanto los diversos ordenamientos jurídicos, como diferentes organizaciones internacionales, han prestado atención al creciente mercado en torno a los datos personales, por lo que se han desarrollado diversas maneras de regularlo, a continuación haremos un breve repaso de los principales modelos que se han adoptado en cuanto a esta materia, con énfasis en nuestra realidad nacional.

2. Regulación en Chile

La regla fundamental respecto al mercado de datos personales en cuanto a las personas y entidades privadas en Chile la encontramos en el Art. 1° de la Ley 19.628, el cual establece como principio de que toda persona puede efectuar el tratamiento de datos personales, mientras lo haga en concordancia con las pautas dadas en la ya mencionada ley y con respeto a los derechos de los titulares de los datos.

Es así como en Chile, en la práctica puede lícitamente generarse un mercado respecto a la información personal, la cual se puede recopilar y transferir fácilmente a terceros, con mínima trazabilidad e injerencia del titular de los datos, existiendo sólo algunos límites específicos, como, por ejemplo, la divulgación a terceros de ciertas categorías de datos.

Dentro de los límites a la divulgación de los datos en razón de su categoría establecidos por esta Ley se encuentra el consagrado en el Art. 17 respecto a los datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial, siendo comunicables sólo en los casos señalados por la ley, hasta por 5 años desde que la obligación se hizo exigible, considerando lo establecido por la Ley 19.812, la cual prohíbe la comunicación de deudas extinguidas al momento de su publicación y aquellas exigibles con anterioridad al 1 de mayo de 2002 que no superen los $2.000.000, la Ley 10.463 la cual limita el

tratamiento de datos de tipo financiero de personas cesantes, y la Ley 20.575, la cual limita la comunicación de estos datos al proceso de evaluación comercial y crediticia. Como puede observarse, el abuso que en la práctica sufrían los particulares por la divulgación de sus datos económicos generó iniciativas legislativas para limitar en forma más detallada su divulgación a terceros.

Otra limitación específica al tratamiento de datos prescrita en la Ley se encuentra en el art. 24, el cual establece reserva sobre las recetas médicas y exámenes de laboratorio clínicos, las cuales solo pueden divulgarse previo consentimiento expreso y escrito del titular.

Otras limitaciones la encontramos en el Art. 154 bis, del Código del Trabajo el que ordena a el empleador a mantener reserva respecto a los datos del trabajador a que tenga acceso con ocasión de la relación laboral y en la prohibición de utilizar los datos electorales con fines comerciales.

Por otra parte, debemos recordar que, en el caso de los datos denominados “sensibles”, su tratamiento está en principio prohibido salvo que (i) la ley lo autorice, (ii) el titular consienta en ello, o (iii) que dichos datos sean necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

En sintonía con lo que hemos podido observar hasta ahora, en Chile la regla general respecto a la comunicación de los datos es que los datos personales puedan ser comunicados con libertad a terceros tanto dentro, como fuera del territorio nacional.

En cuanto a la comunicación de los datos a terceros países, Chile no cuenta con una regulación específica, limitándose a las pautas generales que da la ley para el tratamiento de los mismos, no exigiendo, como hacen otros ordenamientos, que el país receptor cuente con un nivel a lo menos equivalente de protección de los datos personales.

En cuanto a la comunicación de datos dentro de las fronteras del país, esta tampoco está regulada en forma robusta, en desmedro del control de los titulares respecto a su información, considerando las excepciones a la necesidad de contar con su autorización para realizar el tratamiento consagradas en el Art. 6 de la Ley 19.628.

En cuanto al procedimiento automatizado de transmisión de datos, este se regula en el Art. 5 de la Ley 19.628, en los siguientes términos:

Artículo 5º.- El responsable del registro o banco de datos personales podrá establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes.

Frente a un requerimiento de datos personales mediante una red electrónica, deberá dejarse constancia de:

a) La individualización del requirente;
b) El motivo y el propósito del requerimiento, y
c) El tipo de datos que se transmiten.

La admisibilidad del requerimiento será evaluada por el responsable del banco de datos que lo recibe, pero la responsabilidad por dicha petición será de quien la haga.

El receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión.

No se aplicará este artículo cuando se trate de datos personales accesibles al público en general.

Esta disposición tampoco es aplicable cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes.[92]

[92] Artículo 5 de la Ley 19.628.

Finalmente, estamos completamente de acuerdo con Jervis en que "el estado actual de la situación muestra que si bien existen reglas legales que aplican al mercado de datos personales en nuestro país, los datos personales que se comercializan, lo son muy generalmente sin autorización por parte de los titulares de datos respectivos, de manera que éstos no pueden controlar su información personal (cómo, dónde y para qué se utilizará), y, además estos sujetos no son compensados por el uso de la información que les pertenece, ya que las empresas pueden recolectar libremente con la finalidad de utilizar o revelar información en una o múltiples ocasiones que es personal sin tener que pagar ninguna compensación"[93].

3. Regulación en Chile

3.1 Regulación en los Estados Unidos

En los Estados Unidos no existe una ley única y de aplicación general que regule la materia ni una autoridad reguladora específica, sino que un conglomerado de regulaciones sectoriales y estatales[94]. También existen guías y códigos de conducta creados por entidades gubernamentales y gremios, los cuales si bien no son obligatorios, son generalmente aceptados y de gran importancia, por lo que la autorregulación tiene un papel fundamental.

Algunas de las leyes federales más importantes en cuanto a la protección de datos personales son la HIPAA, respecto a los datos de salud, la FACTA, referente a los datos comerciales y de crédito, y la COPPA, la cual protege la privacidad de los niños.

En cuanto a la transferencia de datos personales tanto dentro de los Estados Unidos, como a otros países, existen pocas limitaciones, siendo en general ampliamente aceptada en todos los sectores, salvo en cuanto a que las entidades

[93] JERVIS, Op.Cit., pág. 243.
[94] Vease: JOLLY, Leuan, Data protection in the United States: overview, [en línea] <https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1#co_anchor_a676210> (Consulta: 10 de diciembre de 2018)

estatales deben evitar enviar dicha información fuera de las fronteras del país. Los distintos cuerpos normativos norteamericanos suelen establecer que la legislación de Estados Unidos seguirá siendo aplicable a los datos incluso cuando estos se hayan exportado.

En cuanto a las transferencias con países de la Unión Europea, estas solían basarse en los modelos de contratos aprobados por la Comisión Europea, en el contexto del programa de Puerto Seguro o "Safe Harbour" y en las Normas Corporativas Vinculantes, en el caso de las multinacionales. Sin embargo, el programa de Puerto Seguro fue derogado en el año 2015, en el contexto del caso Schrems contra Facebook[95], lo que llevó a la creación por parte de la Comisión Europea y el Departamento de Comercio de los Estados Unidos de América del marco "Privacy Shield" o "Escudo de Privacidad UE-EEUU", cuya vigencia inició en julio de 2016, para proteger los derechos de los residentes de la Unión cuyos datos se transfieran a los Estados Unidos por motivos comerciales.

Este sistema impone obligaciones para quien realice el tratamiento de los datos, garantías, estándares de transparencia y procedimientos para la protección de los derechos de los titulares, además de un mecanismo de revisión conjunta anual. Así, las entidades norteamericanas que cumplan con lo dispuesto por el marco "Privacy Shield" constaran en un registro. Dada la entrada en vigencia del Reglamento Europeo de Protección de Datos, la adherencia al listado de "Privacy Shield" actualmente no asegura que se estén cumpliendo los niveles de protección de la Unión Europea, por lo que es probable que los criterios para la aprobación[96] de una compañía norteamericana sean reforzados en la próxima revisión anual del programa a fin de compatibilizarlo con la nueva regulación.

[95] Este caso resultó en anulación del programa luego de que el austriaco Maximilia Schrems denunciara ante la autoridad irlandesa de protección de datos a la red social Facebook, por tener esta una filial en dicho país, que sus datos como usuario de la misma, y a raíz de las declaraciones hechas por Edward Snowden sobre el espionaje que realizaría Estados Unidos sobre sus usuarios.

[96] Vease : MUNRO, Olivia, What you need to know about the EU US Privacy Shield and the GDPR, [en línea] <https://www.eci.com/blog/16000-what-you-need-to-know-about-the-eu-us-privacy-shield-and-the-gdpr.html> (Consulta: 10 de diciembre de 2018)

Este sistema se complementa también con la “Judicial Redress Act”, que permite a los ciudadanos de la Unión acceder a acciones civiles en contra del gobierno norteamericano en el caso de que sus derechos se vean afectados.

3.2 Unión Europea

A partir del 25 de mayo del 2018, el instrumento base de la regulación para la protección de los datos personales en Europa es el Reglamento General de Protección de Datos.

Este Reglamento vino a reemplazar a la Directiva 95/46/EC de 1995 y su implementación ha generado gran impacto, no sólo en la Unión Europea, sino que en todo el mundo, siendo actualmente el cuerpo regulatorio más completo y estricto en materia de protección de datos personales, caracterizado por un fuerte énfasis en los derechos de las personas. Por otra parte, por tratarse de un reglamento, resulta de aplicación obligatoria para los Estados miembros.

El gran revuelo causado por el Reglamento se explica porque este resulta aplicable a: a) al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión; b) al tratamiento de datos personales de residentes de la Unión realizado por un responsable o encargado no establecido en la Unión cuando se relaciones con la oferta bienes o servicios hecha a residentes de la Unión Europea o al control de su comportamient**o,** en la medida en que este tenga lugar en la Unión; y c) al tratamiento hecho por un responsable establecido en un lugar donde se aplique el derecho de los Estados miembro de la Unión Europea en virtud del Derecho Internacional Público[97]. Es por esto que prácticamente cualquier entidad, incluso chilena, puede ser eventualmente sujeta al Reglamento, cuyo incumplimiento puede acarrear sanciones hasta por 20 millones de euros o al 4% del volumen de negocio global del último año[98].

[97] Artículo 3 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.
[98] Artículo 83 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

Bajo el Reglamento, para que el tratamiento de los datos personales pueda ser considerado lícito es necesario que cumpla al menos con una de las condiciones señaladas en el Art. 6°, a saber: a) contar con el consentimiento del interesado; b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte; c) es necesario para el cumplimiento de una obligación legal; d) es necesario para proteger los intereses vitales del interesado o de otra persona física; e) es necesario para el cumplimiento del interés público; y f) cuando sea necesario para la satisfacción de intereses legítimos del responsable o un tercero, siempre que sobre estos no prevalezcan los derechos y libertades fundamentales del interesado que requiera la protección de datos personales, en particular si el interesado es un niño. Respecto a los intereses legítimos, quien pretende realizar el tratamiento debe explicarlos al titular de los datos.

El Reglamento también dispone que respecto a los datos personales que revelen el origen étnico o racial de una persona, sus opiniones políticas, religiosas o filosóficas, o la afiliación sindical, así como los datos genéticos, biométricos, de salud, o relativos a su sexualidad, el tratamiento estará prohibido, salvo que se den las condiciones del numeral 2 de su Art. 9°.

Respecto a consentimiento del titular de los datos, será carga de quien realiza el tratamiento probar que este ha sido concedido, en el caso de darse en una declaración escrita esta deberá distinguirse claramente, ser inteligible, de fácil acceso y con un lenguaje claro y sencillo. El consentimiento no podrá ser tácito, y podrá ser revocado en cualquier momento. Asimismo, en el caso en que el consentimiento haya sido entregado sin que el titular de los datos haya tenido una verdadera alternativa de no hacerlo, éste podrá ser considerado inválido.[99]

En cuanto a las transferencias transfronterizas de datos, el Reglamento mantiene el principio de que para proceder a ellas se debe garantizar un nivel de protección equivalente al otorgado por este, ya sea por considerar que el país hacia el cual

[99] Artículo 7 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

se enviaran los datos cuenta con un "nivel adecuado de protección[100]", certificado por la Comisión Europea, o bien si es que el responsable o encargado de transmitir ha ofrecido garantías adecuadas, o cuente con normas corporativas vinculantes aprobadas por la autoridad de control[101].

Finalmente debemos mencionar que el Reglamento robustece la protección de los datos personales a través de las obligaciones impuestas a quienes realizan el tratamiento, de los derechos otorgados a los titulares, tales como el derecho al olvido, a la portabilidad de los datos y a no ser sujeto a decisiones automatizadas incluidas aquellas que se basan en un perfilamiento si estas produce efectos legales y a través del requerimiento de la implementación de sistemas de privacidad por diseño.

Todo lo anterior hace del Reglamento el cuerpo normativo más moderno y robusto actualmente vigente, con una apuesta basada en el titular de los datos y sus derechos y cuya aplicación puede afectar eventualmente a cualquier entidad. Por lo anterior es que los Estados dentro o fuera de la Unión Europea y entidades privadas se encuentran en un proceso de adecuación a esta normativa, por lo que es de esperar que este resulte ser el nuevo estándar global para el tratamiento de los datos personales.

3.3 Autorregulación

Este modelo se define como "aquel que releva a los actores involucrados, empoderándolos en la regulación y control del adecuado de tratamiento de los datos personales"[102], por lo que los agentes del mercado se proveen a sí mismos de un marco regulatorio, las cuales "se manifiestan en instrumentos normativos

[100] Actualmente los estados considerados adecuados son: Andorra, Argentina, Canadá, las Islas Faroe, Guernsey, Israel, la Isla de Man, Jersey, Nueva Zelanda, Suiza, Uruguay. Además se incluye a los Estados Unidos, pero únicamente en lo referente al marco "Privacy Shield".
[101] Artículo 44 y siguientes Reglamento 2016/679 del Parlamento Europeo y del Consejo.
[102] CERDA SILVA, Alberto. 2007. Hacia un modelo integrado de regulación y control en la protección de los datos personales [en línea]. Santiago, Chile: Universidad de Chile. < http://repositorio.uchile.cl/handle/2250/126642> pág.123 (Consulta: 20 de enero de 2019).

que son denominados como códigos deontológicos, sellos de confianza, políticas de privacidad, entre otros."[103]

Para algunos, el propio mercado debe ser el encargado de regular el tratamiento de los datos personales, a través de las mecánicas de la oferta y la demanda, lo anterior lógicamente ha sido ampliamente criticado debido las fuertes fallas de mercado que se dan en el contexto de los datos personales, en particular asimetrías de información en desmedro de los titulares de los datos, sin embargo la autorregulación es un importante factor, especialmente en países como los Estados Unidos en los cuales no existe una regulación comprensiva en la materia. La autorregulación también hace las veces de una regulación supletoria en los casos en que las normativas resultan insuficientes o inaplicables y facilita las transacciones entre diferentes Estados, particularmente en el mundo globalizado en el que vivimos, aportando un marco para las mismas, no limitado por las fronteras territoriales y común para una determinada industria o sector.

Dentro de los límites para esta clase de regulación está que la misma debe ir en concordancia con la legislación existente y que estas solo serán obligatorias para quienes voluntariamente las adscriben, quienes podrán también retirar su adhesión si así estiman conveniente.

En general se trata de normas para una actividad o sector específico, y fácilmente adaptables que se conjugan con la mayor o menor legislación existente en el tema.

En Chile, un ejemplo de autorregulación es el "Código de Buenas Prácticas para el Comercio Electrónico" de la Cámara de Comercio de Santiago, que otorga a las empresas que decidan regirse con él un "sello de confianza ecommerce CCS"[104]

---

[103] RAMÍREZ, Cristóbal. 2015. Protección de datos personales: mecanismos de control preventivos en Chile. Tesis para optar al grado de Licenciado en Ciencias Jurídicas y Sociales. Valdivia, Universidad Austral de Chile, Facultad de Derecho de la Universidad Austral de Chile, pág. 23.

[104] Comité de Comercio Electrónico. [en línea] <http://www.ecommerceccs.cl/sello-confianza-ecommerce-ccs/> (Consulta: 15 de enero de 2019).

y a nivel internacional existen iniciativas como el sello TRUSTe[105], el cual certifica el estándar de privacidad de una compañía en cuanto a sus sitios web, aplicaciones web, plataformas cloud, prácticas de gestión de datos de clientes y trabajadores, cumplimiento normativo y publicidad, y de asociaciones como el sistema Cross Border Privacy Rules de la APEC.

V. Conclusiones.

El tratamiento de los datos personales es una realidad que se da tanto a nivel de instituciones públicas como del sector privado, siendo el Estado el mayor tenedor de datos personales y del cual la ley ha dado algunas directrices para su tratamiento.

En particular, en lo que respecta al tratamiento de datos personales se ha desarrollado sobre la base de que la información se ha transformado en un bien económico transable en el mercado. Dicho mercado de datos personales tiene como consecuencia el desarrollo del mercado de la información personal en el ámbito patrimonial (ej., datos sobre historial crediticio), datos de identificación, datos personales en internet, datos relativos a la salud e incluso datos con fines de marketing.

Por último, podemos ver que la regulación en Chile ha sido débil y en casi ningún caso se cuenta con autorización del titular de los datos personales para su tratamiento. Asimismo, podemos ver que existen otros modelos de regulación del mercado de datos personales como es en Estados Unidos que se ha sustentado sobre la base de una regulación sectorial y autorregulación. Por otro lado, Europa ha dado un salto en cuanto a la regulación con la aprobación de un nuevo reglamento que vino a cambiar las reglas del juego en el mercado de los datos personales.

[105] CERDA SILVA, Alberto. 2006. Algunas consideraciones sobre los códigos de conducta en la protección de los datos personales" Revista Chilena de Derecho Informático, Número 8. 1 enero 2006.

CONCLUSIONES FINALES

El derecho a la vida privada ha experimentado una evolución sistemática la cual ha permitido configurar, a través del avance doctrinario y jurisprudencial, el derecho a la protección de los datos personales, el cual, con el advenimiento del tratamiento automatizado de los mismos ha ganado gran relevancia, alcanzando consagración expresa en nuestra Constitución en el año 2018. Lo anterior se conjuga además, con el desarrollo de otros derechos fundamentales, tales como el derecho a la honra y a la inviolabilidad de las comunicaciones.

Todo lo anterior, a su vez ha permitido configurar el concepto de autodeterminación informativa como una prerrogativa independiente del ser humano que no se circunscribe a amparar a la persona frente al tratamiento de sus datos personales y que revelen circunstancias personales que merezcan permanecer en la esfera privada, sino que, en general, se extiende a todo dato que se predica de determinada persona entregando a esta el control sobre los mismos.

Por otra parte, el rápido avance de la tecnología ha exigido a los distintos ordenamientos jurídicos el desarrollo de una regulación legal y conceptual dedicada a la protección de los datos personales, de modo tal que podemos encontrar en la Ley y la doctrina definiciones que comprenden el concepto de protección de datos personales, sus elementos básicos y asimismo, una serie de principios y derechos que cumplen la función de configurar el marco de protección de los datos personales, así como los procedimientos para asegurar su adecuado tratamiento.

En cuanto a la regulación del tratamiento de los datos personales, esta ha evolucionado de la manos de los cambios sociales y tecnológicos, a través de distintos modelos, tales como la autorregulación y la regulación por vía legal, tal como ha ocurrido en Chile a través de diversos cuerpos normativos, entre los que destaca la Ley 19.628 Sobre la Protección de la Vida Privada, la cual es fuertemente criticada en diversos aspectos, lo que ha desencadenado en diversas

iniciativas legislativas para obtener su modificación, de modo de acercarla al modelo Europeo, actualmente el sistema que mayor protección ofrece a los titulares de datos, considerando además el escenario actual en el cual la tecnología ha permitido que el volumen y variedad de datos tratados, los fines para dicho tratamiento y las posibilidades de afectación de los derechos de las personas a través de este han alcanzado volúmenes nunca antes vistos en la historia de la humanidad.

Así mismo, es posible observar que, en Chile, la regulación respecto al tratamiento de datos personales se ha desarrollado sobre la base de que la información se ha transformado en un bien económico transable en el mercado. Dicho mercado de datos personales tiene como consecuencia el desarrollo de un verdadero mercado de la información personal en el ámbito patrimonial (ej., datos sobre historial crediticio), datos de identificación, datos personales en internet, datos relativos a la salud, los cuales son tratados con diversos fines, entre los cuales destacan los fines de marketing, el cual, en términos generales cuenta con escasa regulación.

BIBLIOGRAFÍA

ANAHIBY BECERRIL, Gil. 2016. Personally Identifiable Information, Big Data y Personal Data Store Personally Identifiable Information, Big Data and Personal Data Store. Revista Iberoamericana De Derecho Informático (Segunda Época). Federación Iberoamericana De Asociaciones De Derecho E Informática. Año 1, N°1.

ALONSO, CARLOS. 2015. OCDE envía carta de advertencia a Chile por retraso en protección de datos personales. [en línea] http://www.pulso.cl/economia-dinero/ocde-envia-carta-de-advertencia-a-chile-por-retraso-en-proteccion-de-datos-personales/

ÁLVAREZ VALENZUELA, Daniel. 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. Universidad Católica del Norte. Año 2013 N°1.

ANAHIBY BECERRIL, Gil. 2016. Personally Identifiable Information, Big Data y Personal Data Store Personally Identifiable Information, Big Data and Personal Data Store. Revista Iberoamericana De Derecho Informático (Segunda Época). Federación Iberoamericana De Asociaciones De Derecho E Informática. Año 1, N°1.

AROS CHIA, Rodrigo Marcelo. 2001. El derecho a la intimidad frente a la sociedad de información. Revista de Derecho de la Universidad Católica de Valparaíso XXII (Valparaíso, Chile).

BANDA VERGARA, A. 2000. Manejo de datos personales. Límite al derecho a la vida privada. Revista De Derecho, 11, 55-70. http://revistas.uach.cl/index.php/revider/article/view/2913.

BANDA VERGARA, Alfonso. La vida privada e intimidad en la sociedad tecnológica actual y futura. Revista de Derecho Público. [En línea] https://revistaderechopublico.uchile.cl/index.php/RDPU/article/view/36294.

BARRERA QUINTANILLA, Tania Isabel. 2013. Estado situacional de la protección de datos personales en Chile, regulación jurídica y alcances. Tesis para optar al grado de Magíster en Gestión de Políticas Públicas. Santiago, Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas.

BARROS BOURIE, Enrique. 1998. Honra, privacidad e información: un crucial conflicto de bienes jurídicos. Revista de Derecho - Universidad Católica del Norte - Sede Coquimbo.

BEYTELMAN, Paloma. 2011. Protección de datos personales en la sociedad de redes. Revista En Foco. ISSN 0717-9987.

CEA EGAÑA, José Luis. 2012. Derecho Constitucional Chileno, Tomo II, Editorial Universidad Católica de Chile.

CERDA SILVA, Alberto. 2003. Autodeterminación informativa y leyes sobre protección de datos. Revista Chilena de Derecho Informático, N°3.

CERDA SILVA, Alberto. 2006. Algunas consideraciones sobre los códigos de conducta en la protección de los datos personales. Revista Chilena de Derecho Informático, Número 8. 1 enero 2006.

CERDA SILVA, Alberto. 2007. Hacia un modelo integrado de regulación y control en la protección de los datos personales [en línea]. Santiago, Chile: Universidad de Chile. < http://repositorio.uchile.cl/handle/2250/126642>

CERDA SILVA. Alberto. 2012. Legislación sobre protección de las personas frente al tratamiento de datos personales. Apuntes de clases, Centro de Estudios de Derecho Informático. Universidad de Chile.

Ciudadanas 2020. EL Gobierno de la información. Coordinadora Patricia Reyes. Instituto Chileno de Derecho y Tecnología. Editorial LOM, año 2011.

COFONE, Ignacio; The way the cookie crumbles: online tracking meets behavioural economics. [en línea] International Journal of Law and Information Technology, Vol. 25, issue 1, <https://doi.org/10.1093/ijlit/eaw013>.

CORRAL, Hernán. EL respeto y protección de la vida privada en la Constitución de 1980. 2001. [En línea] https://corraltalciani.files.wordpress.com/2010/04/vida-privada-y-constitucion.pdf.

ESTEVE, Asunción, The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. [en línea] International Data Privacy Law, Vol. 7, issue 1. <https://doi.org/10.1093/idpl/ipw026>.

GARCÍA, Luis. 1992. Reflexiones sobre la intimidad como límite de la libertad de expresión. EN: Estudios sobre el derecho a la intimidad. Madrid, Editorial Tecnos.

GARRIDO, Romina. 2018, Datos personales e influencia política en Chile". Informe realizado por Derechos Digitales [En línea] <https://datosprotegidos.org/wp-content/uploads/2018/09/Informe-datos-electorales.pdf>.

GUERRERO, Jaime. 1997. La empresa y la magistratura ante la acción de habeas data. Ius et Praxis, vol. 3, núm 1. Universidad de Talca, Talca. Chile.

HERRERA CARPINTERO, Paloma Jesús. 2016. La agencia española de protección de datos descripción y análisis de su rol en la protección a la vida privada y tratamiento de datos personales en las redes sociales. Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile, Facultad de Derecho.

INFORME DE PRODUCTIVIDAD. Proyecto de Ley que Regula la Protección y el Tratamiento de Datos de Personales. Mensaje N°:001-365. Ministerio de Hacienda. 15.03.2017.

JERVIS ORTIZ, Paula. 2003. Derechos del Titular de Datos y Habeas data en la Ley 19.628. Revista Chilena de Derecho Informático.

JERVIS ORTIZ, Paula. 2006. La Regulación del Mercado de Datos Personales en Chile. Tesis para optar al grado de Magíster en Derecho. Santiago, Universidad de Chile, Facultad de Derecho.

JIJENA LEIVA, Renato. 2003. Tratamiento de datos personales en el Estado y acceso a la información pública. Revista chilena de derecho y tecnología. Centro de estudios en derecho informático. Universidad de Chile. ISSN 0719-2576 Vol. 2 Núm. 2 .

JOLLY. Leuan, Data protection in the United States: overview, [en línea] <https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1#co_anchor_a676210>

LAUDON, Kenneth, Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information. [en línea]. NYU Working Paper No. IS-97-04, enero 1997 < https://ssrn.com/abstract=1283008 >.

LETURIA I. Francisco J. Fundamentos jurídicos del derecho al olvido. ¿Un nuevo derecho de origen Europeo o una respuesta típica ante colisiones entre ciertos derechos fundamentales?. Revista Chilena de Derecho, Vol 43 N° 1. año 2016.

MAQUEO RAMÍREZ, María Solange. Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. Revista de Derecho (Valdivia) N°1 Vol XXX- Junio 2017.

MATUS ARENAS, Jessica. 2013. Derecho de acceso a la información pública y protección de datos personales. Revista Chilena de Derecho y tecnología. Centro de estudios en derecho informático. Universidad de CHile. VOL 2 Núm 1.

MONBERG URIBE, Rodrigo. Derecho de Consumo. Revista Chilena de Derecho Privado, N° 28.

MOYA JIMÉNEZ, Paulina Alejandra. 2010. El derecho a ser informado como sustento fundamental del control de datos personales. Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile, Facultad de Derecho.

MORALES, Carlos Alonso. OCDE envía carta de advertencia a Chile por retraso en protección de datos personales. www.pulso.cl Economía y Negocios. jueves 23 de julio 2015.

MUNRO, Olivia, What you need to know about the EU US Privacy Shield and the GDPR, [en línea] <https://www.eci.com/blog/16000-what-you-need-to-know-about-the-eu-us-privacy-shield-and-the-gdpr.html>.

NIMMER Raymond y KRAUTHAUS Patricia, Information as a Commodity: New Imperatives of Commercial Law. [en línea] Law and Contemporary Problems Vol. 55, Summer 1992 < https://scholarship.law.duke.edu/lcp/vol55/iss3/4/>.

NOGUEIRA ALCALÁ, Humberto. Autodeterminación informativa y hábeas data en Chile e información comparativa. [En línea] https://revistas-colaboracion.juridicas.unam.mx/index.php/anuario-derecho-constitucional/article/download/30267/27321 .

OBERG YÁÑEZ, Héctor. Protección de datos de carácter personal. Revista de Derecho. Universidad de Concepción. N°225-226 año 2009. ISSN 0303-9986 (versión impresa).

Protección a los datos personales como derecho constitucional será una realidad. [En línea] http://www.senado.cl/proteccion-a-los-datos-personales-como-derecho-constitucional-sera-una/senado/2018-05-15/181511.html

PICA F, Rodrigo. 2016. El derecho fundamental al olvido en la web y el sistema constitucional chileno, Comentario a la sentencia de protección Rol N°22243-2015 de la Corte Suprema. Centro de Estudios Constitucionales de Chile Universidad de Talca. Estudios Constitucionales, Año 14, N°1.

QUEZADA RODRIGUEZ, Flavio. 2012. La protección de datos personales en la jurisprudencia del Tribunal Constitucional de Chile. Revista chilena de derecho y tecnología. Centro de estudios en derecho informático. Universidad de Chile. Issn 0719-2576 vol. 1 Nro. 1.

RAMÍREZ, Cristóbal. 2015. Protección de datos personales: mecanismos de control preventivos en Chile. Tesis para optar al grado de Licenciado en Ciencias Jurídicas y Sociales. Valdivia, Universidad Austral de Chile, Facultad de Derecho de la Universidad Austral de Chile.

Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado. Santiago, 5 de septiembre de 2011.

Reflexiones sobre el Uso y Abuso de los Datos Personales en Chile. Revista Expansiva. Santiago de Chile, marzo 2011. I.S.B.N: 978-956-8678-04-3.

ROA NAVARRETE, Matías Andrés. 2013. Facebook frente al derecho a la vida privada y la protección de datos personales. Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile, Facultad de Derecho.

ROSTIÓN, Ignacio. 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.

SILVA BASCUÑÁN, Alejandro. 2003. Tratado de Derecho Constitucional Tomo XI. Santiago, Editorial Jurídica,

VIOLLIER, Pablo. 2017. El Estado de la protección de datos personales en Chile. Informe realizado por Derechos Digitales [En línea] <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf>.

LEGISLACIÓN

Ley 19.628 Sobre Protección de la Vida Privada.

la Ley 19.496 Sobre Protección de los Derechos de los Consumidores

Historia de la Ley N° 19.628 Protección de la vida privada. Biblioteca del Congreso Nacional de Chile. D. Oficial 28 de agosto, 1999.

Proyecto de Ley que Regula la Protección y el Tratamiento de los Datos Personales y Crea la Agencia de Protección de Datos personales. [En línea] https://www.carey.cl/proyecto-de-ley-que-regula-la-proteccion-y-el-tratamiento-de-los-datos-personales-y-crea-la-agencia-de-proteccion-de-datos-personales/

Pacto Internacional de Derechos Civiles y Políticos

Convención sobre los Derechos del Niño

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

JURISPRUDENCIA

Sentencia Rol N°11.256-2011 de la Corte Suprema.

Sentencia Rol N°389-03 del Tribunal Constitucional

Sentencia Rol N°1365-09 del Tribunal Constitucional.

Sentencia Rol N°1365-09 del Tribunal Constitucional.

Sentencia Rol N°1732-10-INA y rol N°1800-10-INA (acumulados) del Tribunal Constitucional.

Sentencia Rol N°5243-2015 de la Corte Suprema.

Sentencia Rol N°1.533-2015, de la Corte Suprema.

Sentencia Rol N°4.903-2015 de la Corte Suprema.

Sentencia Rol N°26.932-2015 de la Corte Suprema.

Sentencia del Tribunal de Justicia de la Unión Europea de 19 de octubre de 2016 (Patrick Beyer v. Bundesrepublik Deutschland).

OTROS

Real Academia Española de Lengua http://www.rae.es/

Servicio Nacional del Consumidor. [en línea] <https://www.sernac.cl/app/no-molestar/>