Universidad de Valparaíso.
Facultad de Derecho y Ciencias Sociales.
Escuela de Derecho.

INSTITUCIONALIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES EN CHILE.

(Tesina Carrera Derecho)

Autor: Camila Paz Parra Uribe.

Profesor Guía: Patricia Reyes Olmedo.

Fecha de Entrega: 23 Diciembre 2013.

INDICE

RESUMEN

A partir de un análisis de los derechos fundamentales frente al avance de la tecnología, y específicamente en el ámbito de la protección de datos personales, se analiza la situación de nuestro país, el que pese a disponer de una serie de iniciativas y debates que tratan de cumplir los convenios celebrados y exigencias de la sociedad red, aún no dispone de una institucionalidad adecuada que regule y resuelva los distintos conflictos que se suscitan en esta materia.

Teniendo en vista la necesidad de su existencia, los mecanismos y herramientas en la legislación comparada, se proponen los criterios para la determinación de la institución idónea para la protección de datos personales en nuestro país.

Palabras Claves: Datos Personales – Control – Institucionalidad – Ley 19.628 – Privacidad – Intimidad – Derechos Fundamentales.

INTRODUCCIÓN

El vertiginoso avance de las tecnologías de la información y la comunicación, que queda en evidencia con sólo advertir la masificación de internet, permite una interconexión a nivel planetaria entre personas, grupos de interés, empresas, instituciones, Estados y organismos supranacionales.

La "Sociedad de la Información" hoy por hoy ya no existe, sino que se habla de una "Sociedad Red", término que fue acuñado en 1991, por el holandés *Jan Val Dijk* en su libro *De Netwerkmaatschappij* para definir a una forma de sociedad que se organiza en redes, y son estas redes sociales las que están configurando hoy en día de forma principal la organización y las estructuras más importantes de la sociedad moderna (Reyes Olmedo, Patricia. , 2011), dando paso a un modelo social que se levanta sobre una infraestructura de redes de comunicaciones electrónicas abiertas a las personas las que, a su vez, ejercen su ciudadanía a través de plataformas sociales interdependientes e interrelacionadas, modificando las formas en que tradicionalmente nos relacionamos con nuestro entorno y donde a la vez, la información, el dato, es considerado incluso, hoy en día, como la nueva moneda de cambio.

En este sentido, podemos decir que vivimos y trabajamos en un entorno digital y las estadísticas demuestran fehacientemente que hacemos amplio uso de las redes de información. La información es definida por la RAE como *"La comunicación o adquisición de conocimientos que permiten ampliar o precisar lo que se posee sobre una materia determinada"*, en otras palabras, la información puede ser entendida como el conjunto de datos procesados, que a través de su mensaje, es capaz de cambiar el estado de conocimiento de su receptor. Así visto, es indudable que la información es poder, y que bien o mal utilizada puede involucrar la violación de derechos y libertades considerados fundamentales en cualquier Estado democrático.

Probablemente una de las áreas donde lo anterior tiene mayor significación en nuestro país es en lo que a tratamiento de datos personales se refiere, entendiendo por éste *"cualquier*

operación, complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal o utilizarlos de cualquier otra forma"[1]

Efectivamente, en este ámbito, no existe entre los ciudadanos una real conciencia sobre el procesamiento de información personal que tiene lugar en diversas actividades cotidianas, tales como una compra, o la contratación de un servicio el que implica el registro de nuestros datos personales sin consentimiento explícito de su titular. Tampoco tenemos total claridad respecto a la información recolectada.

En el ámbito internacional sin embargo, el conocimiento y difusión del derecho a la protección de los datos personales ha ido adquiriendo una relevancia creciente y se ha ido incorporando como parte de los temas que deben discutirse. En nuestro país, hasta un poco más de una década se dictó la ley 19.628, titulada "*De Protección a la Vida Privada*", la que no obstante su nombre, se origina en la necesidad de establecer un marco legislativo que permitiera el tratamiento de datos personales; pero ¿esta ha sido totalmente eficaz? ¿Podemos plantear con certeza que con la promulgación de la ley 19.628 nos encontramos en aquella situación donde nuestros datos personales se encuentran protegidos? ¿Existe en nuestro país una institución que regule esto? Si existiese ¿Qué tan distinta es nuestra situación en comparación con otros países? Y si no, ¿Qué tipo de institución sería la más idónea?

En los próximos capítulos se intenta dar a conocer, de modo sintético, un estudio de los derechos fundamentales y su evolución frente a la tecnología, principalmente la protección de datos personales, para luego en el Capítulo II analizar la Ley 19.628 sobre protección de la vida privada, posteriormente analizar la institucionalidad de control y finalizar con un análisis de la situación en distintos países respecto a la institución de control presente en éstos.

[1]Articulo 2 Ley 19.628; Texto disponible en http://bcn.cl/4fu9 (Consultada diciembre 2013)

CAPITULO I

LAS BASES DE LA PROTECCIÓN DE DATOS PERSONALES.

1.- Los derechos fundamentales frente a la tecnología.

Los derechos fundamentales pueden ser concebidos desde dos ópticas: por un lado, como ciertos dictámenes de justicia subjetivizados, a los que se reconoce, por un motivo u otro, una importancia fundamental para la vida del hombre en razón de la relevancia de los objetos o materias a que se refieren, y por el otro, desde un punto de vista jurídico positivo, como ciertos atributos legales en cuanto son conferidos no por cualquier ley ordinaria, sino por la Constitución. (Muñoz, 1998, p. 27)

Su expresión como derechos fundamentales es relativamente reciente, surgida hacia 1770 en los *droits fondamentaux* de Francia, dentro del movimiento que condujo a la Declaración de los Derechos del Hombre y del Ciudadano, de 1789, y que, según explica Pérez Luño, constituye la fase más avanzada del proceso de positivización de los derechos naturales en los textos constitucionales del Estado de Derecho. (Perez, 1995, p. 29)

Sin duda, el factor histórico resulta determinante para conocer y comprender el catálogo de derechos fundamentales de una sociedad democrática en particular. En la actualidad estos presentan distintos rasgos que permiten hablar de una tercera generación de derechos humanos, complementaria de dos fases anteriores.

La primera generación se refiere a las libertades individuales y sus derechos de defensa a través de la autolimitación y la no injerencia de los poderes públicos en la esfera privada. La segunda generación representa derechos de participación que requieren de políticas activas de los poderes públicos encaminadas a garantizar su ejercicio, es decir, son derechos de tipo económico, social y cultural. Y la tercera generación de derechos fundamentales está estrechamente vinculada a la sociedad tecnológica, en su calidad de derechos positivos, por lo que ya no pueden calificarse de “innatos”. (Herrera Bravo, 2001, p. 2)

Respecto de los derechos fundamentales de tercera generación, a través de un análisis funcional de los derechos fundamentales, es posible distinguir dos cometidos complementarios (Perez, Antonio; Losano, Mario; Guerrero, Maria Fernanda, 1989, p. 144): por una parte, reconocen determinadas facultades o posibilidades de actuación a los ciudadanos, y por la otra, propenden hacia un equilibrio de poderes políticos, sociales y económicos al interior de las sociedades democráticas a que pertenecen. Si esas sociedades presentan un nivel de desarrollo tecnológico importante, es posible prescindir cada vez más de la coacción física, para dar paso a complejas amenazas a los derechos y libertades mediante el uso de la información para influir y controlar la conducta de las personas.

La convivencia en justa libertad al interior de una sociedad democrática, provoca que estos derechos tengan límites que, lejos de imponerles una carencia, los dimensiona y precisa. Por una parte la dignidad de la persona es uno de los criterios para la delimitación de estos derechos, ya que se considera como la fuente de obligatoriedad del derecho configurado para cualquier acción limitadora del Estado.

Otro límite se encuentra en el respeto y tolerancia al ejercicio de los derechos de terceros, especialmente los que se derivan de la propia naturaleza del derecho, de la existencia de otros derechos que eventualmente pueden entrar en conflicto con el que se invoca; o de circunstancias temporales, personales u objetivas.

En definitiva, los derechos fundamentales gozan de un régimen de protección jurídica reforzada, manifestada en una serie de diversos instrumentos de tutela, dentro del que destacan las garantías normativas. A través de ellas, la Constitución busca asegurar su cumplimiento, evitar su modificación y mantener la integridad de su sentido y función.

2.- La protección de los datos personales como derecho fundamental.

2.1 - Los primeros pasos: Privacy norteamericana.

El derecho a la protección de datos personales ha recorrido un largo camino hasta adquirir la forma que hoy conocemos, siendo una de las primeras fórmulas jurídicas para protegerse de las distintas agresiones de la informática el buscar refugio en la antigua institución de

Derecho norteamericano conocida como "*privacy"*, cuyos orígenes se remontan a la formulación que hicieran de ella Louis Dembitz Brandeis y Samuel Dennis Warren, la cual elaboraron a partir de precedentes jurisprudenciales y publicaron como *"The Right of Privacy"*[2]; esto es, un derecho concebido como *"The right to be let alone", "el derecho a ser dejado solo"*, a no ser molestado, lo que conlleva como consecuencia la negación de la posibilidad de controlar la información que pertenece a la persona por el hecho de emanar o referirse a ella.

Aunque la *privacy* es la fórmula que permitió al derecho norteamericano enfrentar la capacidad invasiva de las tecnologías, este es un concepto que en su origen no tiene relación alguna con la informática, sino que fue ideado en el siglo XIX como un escudo o límite a la intromisión de los periódicos y la prensa en general en la vida de las personas. (Reusser, n.d., p. 2)

Hoy en día, la *privacy* norteamericana ha ido ampliando de manera constante sus contornos por vía jurisprudencial hasta incluir la protección de los datos de las personas en relación con la informática. La *privacy*, ha derivado en un derecho constitucionalmente protegido, aun cuando la Constitución no lo reconoce expresamente, no lo delimita ni lo define, sino que la doctrina y la jurisprudencia lo sustentan en el contenido de la IV enmienda[3].

2.2.- "Riservatezza" italiana.

Los sistemas de derecho continental no poseían ninguna figura semejante a la *privacy*, sin embargo, manejaban dos conceptos fuertemente enraizados, como son la intimidad y la *riservatezza* (reserva). En su momento se vio como la solución más sencilla equiparar intimidad y reserva con privacidad, la cual parecía lo suficientemente elástica y amplia como para servir a este fin. Sin embargo, tanto la intimidad como la reserva tienen una naturaleza diferente, son conceptos definibles a priori y determinados, pues intimidad es "la zona espiritual íntima (interna) de una persona" y la reserva es el "modo de ser de la

[2]Disponible en: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (Consultada Diciembre 2013)
[3]Texto disponible en: http://www.archives.gov/espanol/constitucion.html (Consultada Diciembre 2013).

persona que consiste en la exclusión de los otros del conocimiento de cuanto se refiere a la persona misma".(Reusser, n.d., p. 5)

El concepto de *privacy,* fue acogido en este medio porque cuando se descubren los peligros de la acumulación de datos para los derechos fundamentales y su falta de previsión constitucional, se mira a esta institución como una herramienta efectiva para cubrir el vacío existente en la protección de datos, sin embargo, la transforman, ya queentienden que se refiere sólo a la protección de derechos frente a la informática y el resto de los contenidos se subsumen en los derechos fundamentales correspondientes al sistema continental europeo.

Sin embargo y luego de los distintos problemas que han surgido a partir de otorgar a instituciones jurídicas nombres que no les corresponden, autores como Mario Losano y Frosini, han manifestado que la *riservatezza* no es el instituto jurídico adecuado a las necesidades que genera la protección de datos, ya que lo que se encubre con este concepto ampliado es tomar la *privacy*, eliminar algunos contenidos de esta y luego generar equivalencias o que incluso son identificables con la reserva.

Lo que claramente reconoce el texto italiano son varias formas concretas de la "reserva", como el domicilio, las comunicaciones y algunos aspectos de la libertad y del pensamiento como derechos inviolables, cuya defensa se organiza con criterios negativos, pero no existe un derecho constitucional a la *riservatezza*que proteja de forma global todas las facetas privadas de la persona. (Reusseur Monsálvez, n.d., pp. 6 - 7)

2.3.- Alemania y el Derecho a la Autodeterminación Informativa.

En Alemania, se ampara la dignidad de la persona y la personalidad lo que les ha permitido construir el *Recht auf informationelle Selbstbestimmung*[4], a través de una sentencia[5] del Tribunal Constitucional Federal que declaró como violatorio de la intimidad algunos preceptos de la Ley de Censo de 1982. Esta sentencia, independiza la protección de datos

[4] Derecho a la autodeterminación informativa.
[5]Sentencia citada por Prieto Gutiérrez, Juan José. "Protección de datos en la Biblioteca de la Universidad Complutense", 2006. Disponible en: http://www.scribd.com/doc/42380514/Proteccion-de-Datos-en-La-Biblioteca-de-La-Universidad-Complutense-de-Madrid,.

personales respecto de la intimidad, el honor y la propia imagen como garantías protegidas y recalca la función instrumental a la protección de la dignidad, la igualdad y la libertad que asisten a la persona humana en general, de las que derivan la generalidad de las garantías consagradas en los distintos catálogos de derechos. Este derecho le faculta para decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida, de lo que se deduce la "libre eclosión de la personalidad del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona".(Murillo, 1990, p. 121)

La autodeterminación informativa entonces es el derecho del individuo de controlar la obtención, tenencia, tratamiento y transmisión de datos relativos a su persona, decidiendo en cuanto a los mismos las condiciones en que dichas operaciones pueden llevarse a cabo. (Reusser, s.f., p. 9)

2.4.- La Intimidad: La principal vía europea.

El sistema europeo no inicia la construcción de la protección de datos a partir de la reserva, sino que a partir del derecho a la intimidad, del derecho al honor y a la propia imagen, los que fueron cobrando relevancia atendido el avance del desarrollo tecnológico y su capacidad invasiva.

De hecho, es esta corriente la que da lugar a las primeras manifestaciones normativas de la protección de datos, ya en 1981, a través del Convenio 108 del Consejo de Europa[6], se reconoce expresamente la necesidad de garantizar la intimidad de las personas, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos personales que son objeto de tratamientos automatizados. (Reusseur Monsálvez, n.d., p. 7)

A partir del pronunciamiento del Constitucional Alemán y la configuración de la Autodeterminación Informativa, como un derecho autónomo, y más tarde el Tribunal Constitucional Español, en 1990, hiciera lo propio, bajo la denominación "libertad

[6]Convenio 108 "para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal" Texto disponible en: http://www.coe.int/t/dghl/standardsetting/dataprotection/Global_standard/Conv%20108_es.pdf (Consultada diciembre 2013).

informática" se ha ido configurando la base de este nuevo derecho, que en definitiva se sienta sobre tres bases concretas (Donoso, 2013, pp. 90 - 91):

1) El reconocimiento de que las personas a que se refieren o conciernen los datos personales son sus únicos "dueños" y por ende la imposibilidad de que los terceros que los recogen, almacenan y en general, que realizan operaciones de tratamiento, adquieran el dominio de estos datos, sino que a lo más serán sus custodios. Del mayor o menor desarrollo de este eje dependerá el régimen de responsabilidad que se defina en un Estado determinado.

2) La convicción de que todo dato personal es relevante y por tanto ha de protegerse respecto de su tratamiento por terceros, distinto de su titular. Esto sin perjuicio de reconocerse que existen datos más sensibles que otros. El desarrollo de este aspecto conlleva la configuración legal del derecho a tratar datos de terceros y el encasillamiento de cada tipo de dato personal en cada una de las categorías que se definan (datos de libre acceso al público, datos sensibles, etc.).

3) Como consecuencia de las dos bases anteriores: los titulares de los datos deben, en todo momento, poder controlar el uso que los terceros hacen de los datos personales que le conciernen. Esta es la base sobre la cual se desarrollan los distintos derechos que se reconocen al titular de datos personales, usualmente conocidos como derechos ARCO, esto es, Acceso, Rectificación, Cancelación y Oposición al tratamiento de datos personales.

Así, ha surgido una abundante normativa que acompaña el proceso de consolidación de este derecho y que va reflejando los giros legislativos y las experiencias de los países. Dentro de este contexto, debemos mencionar las "Directrices para la regulación de los archivos personales informatizados", adoptadas por las Naciones Unidas mediante resolución 45/95[7], de la Asamblea General, de 14 de diciembre de 1990, y a nivel europeo, la

[7]Texto disponible en: http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/572/58/IMG/NR057258.pdf?OpenElement (Consultado diciembre 2013).

Directiva europea 95/46/CE[8], del Parlamento y del Consejo, de 24 de octubre de 1995. Y la consagración en la Carta de los Derechos Fundamentales de la Unión Europea, proclamada en diciembre del 2000[9]". (Reusseur Monsálvez, n.d., p. 12).

3.- El Derecho a la vida privada en Chile.

3.1.- El Derecho a la vida privada en la Constitución Política de 1980

La Constitución Política de la República de Chile, en su artículo 19 número 4[10], asegura a todas las personas el respeto y protección a la vida privada y pública y a la honra de la persona y de su familia. Y es el párrafo siguiente del mismo artículo el que se refiere al honor o a la honra. En cambio, el artículo 19 número 5, alude claramente a la vida privada cuando asegura la inviolabilidad del hogar y de toda forma de comunicación privada.

Teniendo estos dos artículos en vista, Desantes manifiesta tres consideraciones que siendo generales, pueden apoyarse en la propia Ley Constitucional de Chile:(Desantes, 1992, p. 269)

1) El derecho a la intimidad es un derecho innato del hombre. El artículo 5 de la Constitución reconoce la existencia de derechos esenciales que emanan de la naturaleza humana; por lo que son superiores a la propia Ley constitucional estén o no citados en ella e inalterables legalmente. Por el contrario, el ejercicio de la soberanía ha de considerarlos como limitación; y a los órganos del Estado se les impone el deber de respetarlos y promoverlos. El derecho a la intimidad no aparece citado expresamente entre tales derechos; si el derecho a la vida privada y el derecho a la libertad de conciencia, en el artículo 19 número 6, que aunque no la agota, forma parte de la intimidad.

2) Las modernas constituciones, se han convertido en los conductos por los que se incorpora al ordenamiento jurídico interno el Derecho Supranacional, lo que constituye un importante factor de homogenización a la hora de comparar los diferentes ordenamientos.

[8]Texto disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML (Consultado diciembre 2013).
[9]Texto disponible en: http://www.europarl.europa.eu/charter/pdf/text_es.pdf (Consultado diciembre 2013).
[10] Texto disponible en: http://bcn.cl/1hsz7 (Consultado diciembre 2013).

Los derechos humanos no solamente están reconocidos en la Constitución, sino también, según el mismo artículo 5° de la propia Carta Fundamental, en los tratados internacionales ratificados por Chile y que se encuentran vigentes.

3) La protección de la vida privada constituye una clara tendencia en los documentos supranacionales, a partir de la misma Declaración Universal de Derechos Humanos de 10 de diciembre de 1948 artículo 12 y de las legislaciones internas más modernas, como la francesa. La constitución chilena, en esta misma línea, asegura el respeto y protección al derecho a la vida privada de la persona y de la familia.

El artículo 19 número 26 de nuestra Carta Fundamental[11] consagra el denominado contenido esencial de los derechos; esta garantía constituye un límite o frontera que no se puede transgredir, vale decir, se asegura a todos los individuos de nuestra sociedad el respeto al núcleo o esfera básica de cada derecho, sin el cual sería impracticable.

El tema de la vida privada e intimidad, se aborda en nuestro texto constitucional chileno asegurándolo como un solo derecho en conjunto con la honra, en circunstancias que se trata de derechos conceptuales y realmente distintos (Desantes, 1992, p. 268). Nuestra Constitución no define lo que deba entenderse por "vida privada" ni pormenoriza cuáles serían los contenidos en que pudiera desglosarse tal derecho, como lo hacen otros textos constitucionales. Forma parte, asimismo, de la protección constitucional a la intimidad, otro derecho asegurado por Ley Fundamental, cual es el referido a la libertad de conciencia, de modo que nuestro constituyente ha desglosado de la manera antedicha los derechos que tutelan la vida privada o intima de las personas.(Banda Vergara, 2000, p. 61)

El derecho a la protección de la vida privada consiste en la facultad de las personas a mantener un ámbito de su vida fuera del conocimiento público, en el cual desarrolla acciones que se inician y concluyen en el sujeto que las realiza, como así mismo concreta relaciones francas, relajadas y cerradas que trascienden sólo a la familia o aquellos con los que determina compartir, siempre y cuando tales actuaciones y relaciones no dañen a otros,

[11] Texto disponible en: http://bcn.cl/1hsz7 (Consultado diciembre 2013).

no sean delitos o no sean hechos de relevancia pública o que afecten al bien común. En este ámbito los terceros sólo pueden entrar con el consentimiento de la persona afectada.(Nogueira Alcala, 2004, p. 124)

En la Comisión Constituyente no se trató de definir el concepto de vida privada(Banda Vergara, 2000, p. 61), dejando su concreción a la jurisprudencia, donde encontramos que ha sido acogida la definición del profesor Cea Egaña (Cea Egaña, 1996, p. 27), en la sentencia del caso Martorell (Martorelli - Editorial Planeta., 1993); sosteniendo que se viola la vida privada y origina las sanciones que establezca la ley, la intrusión indebida y maliciosa en asuntos, comunicaciones o recintos íntimos que el titular del bien jurídico o protegido no desea que sean conocidos por terceros sin su consentimiento, se cause o no con tal motivo sufrimiento o daño al afectado.

Es importante señalar que nuestra Constitución se ocupa de estatuir que la infracción de este derecho a la intimidad, 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, por lo que existe una cierta disponibilidad del legislador por regular, limitar o restringir su ejercicio.

3.2.- Bienes jurídicamente protegidos.

Suele afirmarse que el abuso de las tecnologías de información y comunicaciones constituye la amenaza por excelencia contra la intimidad, debido a que cruzándose telemáticamente datos personales o nominativos puede obtenerse un perfil de las personas cuyos antecedentes son procesados.

El problema de fondo se origina por un conflicto entre el legítimo interés de aquellas personas cuyos datos nominativos se procesan computacionalmente, en resguardar su vida privada y la necesaria confidencialidad de antecedentes como sus creencias religiosas, su filiación política, sus tendencias sexuales, su estado de salud, el monto de su patrimonio, etc. Mientras, que por otro lado, hay también un interés legítimo que poseen los gobiernos y los particulares para acceder a cierta información, ya que los Estados para poder cumplir

con sus fines promocionales y asistenciales de orden público, como por ejemplo, saber quiénes tienen determinadas enfermedades para fijar políticas de salud, o para asegurar la vigencia de un orden público económico necesitarán conocer los antecedentes comerciales irregulares o negativos de las personas que actúan en la vida comercial. (Jijena Leiva, 2001, p. 87) El límite entre la esfera privada y la esfera social o pública de una persona no se ha establecido legalmente con claridad.

En nuestro país, dichos datos, están protegidos por la esfera íntima que consagra la garantía del artículo 19 número 4 de la Constitución; asegurando a todas las personas el derecho a la intimidad; asegurando tres dimensiones del derecho, siguiendo lo mencionado por Humberto Nogueira(Nogueira Alcala, 1998, p. 68)

1) El derecho al respeto de la vida privada de las personas.
2) El derecho al respeto de la vida pública de las personas.
3) El derecho al respeto de la honra de las personas y de su familia.

El respeto implica la obligación de terceras personas, sean naturales o jurídicos, públicos o privados, en orden a no interferir en el ámbito del valor y conducta protegido jurídicamente, el cual recibe la protección del Estado a través del conjunto de garantías que brinda a tales bienes jurídicos y a sus titulares para defenderlos y exigir que ellos sean respetados.

Este respeto y protección, debe desarrollarse en relación con la "vida privada" de la persona y la "vida pública" de ella.

La Constitución de 1980, en su artículo 19 número 4, al asegurar el derecho a la vida privada de la persona protege también la intimidad corporal frente a toda indagación o investigación que sobre el cuerpo de la persona quisiera interponerse contra su voluntad, protegiendo su pudor de acuerdo a los criterios vigentes en la cultura y la moral de la sociedad, salvo que tal afectación al ámbito de la intimidad sea por decisión judicial que tendrá que proveer que la ejecución sea respetuosa de la dignidad de la persona y no constitutiva de trato degradante. Otro ámbito importante es la intimidad sexual de las personas, así se reconoce el derecho a que se mantenga reservado un ámbito de comportamiento, ya sea de conductas, preferencias sexuales, o, lo que se ha denominado, el

derecho a la propia imagen, que es el derecho de impedir que otros capten o difundan dicha imagen sin su consentimiento, teniendo como único limite la moral o las buenas costumbres o la ley. (Nogueira Alcala, 1998, p. 70)

La norma constitucional, para concluir, asegura a todas las personas el respeto de los aspectos más profundos o reservados de ella, sin que sea posible la intromisión en su esfera, salvo que medie autorización de su titular. Asimismo se aseguran a todas las personas las defensas que poseen para proteger su intimidad frente a los posibles ataques que puedan sufrir.

CAPITULO II

LA LEY N° 19.628 SOBRE PROTECCION DE LA VIDA PRIVADA

1.- Antecedentes.

En Chile, desde sus orígenes, la protección de los datos personales ha estado vinculada al derecho a la privacidad. Un ejemplo de ello, es el desarrollo legislativo que ha tenido la materia en nuestro país, cuyo tratamiento lo podemos encontrar fundamentalmente en la ley 19.628, de 1999,[12] sobre protección de la vida privada. En ella, la protección de datos nace concebida como parte del derecho de las personas a ser dejadas solas.(Arrieta, 2009, p. 13).

Además, se reconoce en el proyecto que las regulaciones establecidas de la vida privada, y que dada la dispersión de normas existentes sobre la materia, se hace necesaria la dictación de un cuerpo normativo específico y sistematizado sobre la vida privada.

Por otro lado, en lo que respecta específicamente a la protección de datos personales, en el título segundo de dicho cuerpo normativo, se establecen algunos principios generales que deben regir la materia.

En cuanto a la responsabilidad por las infracciones a la ley, se establecen procedimientos de reclamación ante los tribunales civiles, así como también los mecanismos necesarios para que las personas afectadas persigan las indemnizaciones respectivas en caso de daños, sin perjuicio de poder también recurrir ante los tribunales superiores mediante acción de protección por vulneración de la garantía fundamental establecida en el artículo 19 número 4 de la Constitución, es decir el derecho a la vida privada y a la honra de toda persona. (Castro Martines, Karla. Moreno Carrasco, Diego, 2012, p. 472)

2.- Definiciones legales.

Si bien nuestro legislador estimó necesario contemplar distintas definiciones legales, es necesario tener en cuenta que el Diccionario de la Real Academia Española define a los

[12] Texto disponible en: http://bcn.cl/4fu9 (Consultado diciembre 2013)

"datos" como el "Antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legitimas de un hecho."[13].

Oscar Pucinelli, agrega a esta idea que el vocablo dato alude a un elemento circunscrito y aislado, que no alcanza a tener el carácter de información, pues para que se transforme en ella se requiere la interconexión de esos datos de manera que, vinculados, se conviertan en una referencia concreta.(Pucinelli, 1992, p. 27). El *"dato*", para significar y tener contenido, deberá acompañarse de una referencia intencional, de manera que tienda hacia algo y lo relacione otorgándole sentido. Es decir, para existir últimamente, para que tenga vocación de información, debe contener una referencia a un sujeto, una persona u objeto o cosa, de manera tal que nos permita conocer a ese alguien o algo.(Bahamonde Guasch, 2008, p. 8).

El dato será *"personal"* cuando contenga una referencia dada por un elemento circunscrito y aislado que permita individualizar a una persona determinada o determinable, aludiendo a la definición que nos entrega la ley 19.628 en su artículo 2 letra f)[14]. Siguiendo a Ekmekdijan y Pizzolo (Ekmekdjlan, Miguel Angel y Pizzolo, Calogero., 1995, p. 64); el aludir a la formula "determinada o determinable o bien identificada o identificable", tiende a dar un tono amplio a la configuración del concepto, materializando un principio hermenéutico del derecho constitucional que prescribe que los derechos individuales y las garantías creadas para proteger a estos, deben ser interpretados con un sentido amplio, por lo que se hace extensiva a todos aquellos individuos que pueden llegar a ser identificados por medio de datos.

La ley 19.628 entrega un concepto legal de *"datos de carácter personal o datos personales"* en su artículo 2 letra f)[15], entendiendo por ellos, "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables"; se sigue un criterio amplio y con efectos parciales, circunscritos sólo a su ámbito de aplicación y considerando como titulares de datos personales, sólo a las personas naturales.

[13]Diccionario de la Real Academia Española, texto disponible en: http://lema.rae.es/drae/?val=dato (Consultada diciembre 2013)
[14]Ley 19.628, texto disponible en: http://bcn.cl/4fu9 (Consultada diciembre 2013)
[15]Ley 19.628, texto disponible en: http://bcn.cl/4fu9 (Consultada diciembre 2013)

Los amplios términos con que la ley conceptúa los datos personales permiten afirmar que no sólo se refiere a contenidos en formato de texto, sino que comprende también, documentos en formato imagen y sonido, con tal que transmitan información, concerniente a personas susceptibles de ser identificadas. De este modo, desde que el dato puede ser asociado a una persona, la condición de identificación queda satisfecha y el régimen jurídico a que queda afecto su tratamiento es el previsto en la ley 19.628. (Cerda Silva, 2003, p. 76).

A partir del concepto de *"datos personales"* podemos distinguir éste de otros conceptos, como es el caso de los *"datos públicos"*, que si bien pueden estar relacionados con la información personal, se relacionan también con el derecho a la información pública o el derecho fundamental a la información. También se distinguen sus sub clasificaciones, la ya señalada de *"datos personales públicos y datos personales privados"*; y otras como *"datos nominativos","datos patrimoniales o económicos";* que no serán objeto de discusión en este análisis.

Dentro de las definiciones se puede destacar la de *"datos sensibles",* que 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", aunque la discusión en la doctrina respecto a éstos no es conteste ya que para algunos autores, no tiene sentido ahondar en la distinción entre *"datos sensibles o no sensibles"*, pues incluso los que pudieran ser considerados como irrelevantes o inocuos pueden convertirse en sensibles dado el uso que se haga de los mismos. Sin embargo, debemos comprender que este tipo de datos, afecta directamente el ámbito reservado del individuo, su esfera privada y en tanto su manejo irroga un mayor riesgo en la dignidad e intimidad de la persona, se requiere sobre ellos una protección más estricta.

Respecto a los *"registros o banco de datos"*, que conforme al artículo 2 letra m) de la Ley 19.628, son el "conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar

los datos entre sí, así como realizar todo tipo de tratamiento de datos" podemos plantear que aun cuando, se disponga de un conjunto organizado de datos personales, si estos no pueden ser relacionados entre sí o realizar operaciones de tratamiento a su respecto, no constituirán un banco de datos para los fines de la ley 19.628.

3.- Ámbito de aplicación.

3.1.- Ámbito material de aplicación.

La ley 19.628, extiende sus efectos a aquel tratamiento de datos de carácter personal verificado en forma automatizada y manual, lo cual queda de manifiesto al definir *"tratamiento de datos*" en el artículo 2 letra o), como "cualquier operación o complejo de operaciones o procedimientos técnicos de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma".

Como corolario y estableciendo una especie de principio de legalidad o una especie de condición general de licitud para este ámbito, el artículo 1° agrega que cualquier persona podrá efectuar el tratamiento de datos personales siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico, y que en todo caso, se deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce(Jijena Leiva, 2001, p. 94). Asimismo, la propia ley se ha encargado de precisar el concepto de ciertas operaciones de que pueden ser objeto los datos, tales como almacenamiento, bloqueo, comunicación o transmisión, eliminación o cancelación, modificación y disociación de datos.

3.2.- Ámbito subjetivo de aplicación.

A. Titular de datos personales.

El titular de datos personales, conforme al artículo 2 letra ñ), es sólo la persona natural por lo que las personas jurídica, que si bien también poseen atributos de su personalidad, por definición quedan al margen de la ley.(Jijena Leiva, 2001, p. 94)

La ley no define al titular en términos de establecer un derecho de propiedad entre él y los datos que le conciernen, sino que atiende a una circunstancia de hecho, cual es que se refiera a información relativa a su persona, con ello se sortean las dificultades que en doctrina se suscitan en torno a quien compete la propiedad sobre la información contenida en bases de datos nominativos, si al responsable de la base o a quien los datos se refieren.(Cerda Silva, 2003, p. 79).

B. Responsable del registro o banco de datos

La ley distingue lo que es el procesamiento de datos personales al interior de la Administración Estatal o en el Sector Público y lo que ocurre en el sector privado o respecto al tratamiento por particulares, sean estas personas naturales o jurídicas. La gran mayoría de las leyes de protección de datos en el derecho comparado establecen una clara diferenciación entre las bases de datos públicas y las privadas, en atención a la naturaleza de la entidad que las administra y no, como lo hace la ley chilena, en consideración a la fuente de la información o al tipo de datos procesados.(Jijena Leiva, 2001, p. 95)

Nuestra ley califica como responsable del banco de datos a aquel en quien recae la adopción de decisiones relativas al tratamiento de los datos personales, y admite que pueda tratarse tanto de una persona natural o jurídica privada, e inclusive un organismo público (Artículo 1 y 2 letra n)[16]. Más aun, la ley se ha encargado de precisar que, para efectos de lo dispuesto en ella, se entenderá por organismo público, las autoridades, órganos del Estado y organismos descritos y regulados por la Constitución Política de la Republica, y los comprendidos en el inciso segundo del artículo 1 de la Ley 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.(Cerda Silva, 2003, p. 81)

4.- Los principios relativos al tratamiento de datos.

La ley 19.628, se encuentra inserta en el marco de nuestro ordenamiento jurídico y por consiguiente queda sujeta a distintos principios generales del derecho, pero a la vez, según señala Cerda Silva(Cerda, 2006), esta ley contempla ciertos principios específicos en relación con el tratamiento de datos.

[16]Ley 19.628, texto disponible en: http://bcn.cl/4fu9 (Consultada diciembre 2013)

En primer lugar, la libertad en el tratamiento de datos personales. El artículo 1 de la ley 19.628, asegura que toda persona puede efectuar el tratamiento de datos personales; sin embargo, condiciona su ejercicio a que se adopten distintos resguardos, tales como que el tratamiento de datos debe hacerse de manera concordante con la ley, las finalidades del tratamiento deben ser permitidas por el ordenamiento jurídico, entre otras. (Donoso, 2013, p. 89)

El segundo principio recae en la información y el consentimiento del titular reflejado en el artículo 4 de la ley 19.628, donde además del consentimiento expreso de su titular, el tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen. Si bien la regla general es que se exija consentimiento del afectado por el tratamiento de datos, la ley prevé algunas excepciones. En primer lugar, la ley permite que exista un tratamiento de datos personales aún sin el consentimiento del interesado en casos tales como cuando se trata de datos de carácter económico, financiero o comerciales extraídos de fuentes accesibles al público y que se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión, títulos educativos, etc. Tampoco es necesario el consentimiento cuando se trate de un tratamiento de datos efectuado por personas jurídicas privadas, para el uso exclusivo suyo, de sus afiliados y que sea realizado con fines estadísticos u otros fines de beneficio general de aquellos. (Donoso, 2013, pp. 96 - 97):

El tercer principio es el de la finalidad, el que recae en que los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, con la excepción de aquellos datos que provengan o se hayan recolectado de fuentes accesibles al público, artículo 9 Ley 19.628.

Respecto a la calidad de los datos, que se configura como el cuarto principio, tanto la doctrina como la legislación comparada expresan que el tratamiento de los datos personales está informado por este principio. Si consideramos que la protección de la persona frente al tratamiento de datos personales, afecta derechos fundamentales o incluso puede llegar a constituirse en una garantía autónoma, entonces, las actividades de tratamiento de datos

personales se rigen por el principio de legalidad y por tanto deben cumplir una serie de condiciones en el tratamiento de datos personales, tales como que exista autorización legal para realizar tratamiento de datos personales, que se trate de datos verídicos y vigentes en cada momento y que sean datos adecuados, pertinentes y no excesivos.

El quinto principio, está relacionado con que no todos los datos personales, merecen el mismo grado de resguardo para el legislador, ya que no todos ellos suministran una información de igual relevancia; tanto es así, que la ley hace una enumeración, del tipo enunciativa, de datos que estima sensibles mencionando aquellos relativos a 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.(Donoso, 2013, p. 98)

El deber de secreto, es el sexto principio, éste recae tanto sobre el responsable del banco, como sobre las personas que intervienen directamente en el tratamiento de los datos; y se refleja asimismo en el artículo 7 de la ley en comento.

Por último, la temporalidad, es el séptimo principio relevante. La normativa internacional en general es conteste en señalar que no puede existir un tratamiento de datos personales que contenga datos "históricos"; lo que se refleja en el artículo 28 de nuestra ley.

5- Los derechos del titular de datos personales.

Los derechos de los titulares de datos reconocidos en la ley 19.628, son básicamente cuatro: (Jervis Ortiz, 2002, p. 20)

5.1.- Derecho de Información o Acceso.

Toda persona tiene derecho a exigir del órgano o servicio que sea responsable de un banco de datos, información sobre los datos relativos a su persona, su procedencia y destinatario. (Rajevic Mosler, 2011, p. 7). Este derecho lo podemos conceptualizar como aquel que posee todo titular de datos para exigir del responsable del banco de datos ya sea privado o público, información que le permita saber si se tratan datos suyos y, de ser así, cerciorarse de su exactitud y de la licitud de su tratamiento.

5.2.- Derecho de modificación.

Ante el evento que los datos contenidos en la base dejen de responder a la situación real, o bien haya cesado la legitimidad de su tratamiento, el titular de estos, tiene derecho a que ellos sean modificados de manera que reflejen con precisión la circunstancia que pretenden En contrapartida, la ley se encarga de establecer para el responsable del banco, la obligación de modificar los datos, sin necesidad de requerimiento del titular. (Cerda Silva, 2003, p. 100)

5.3.- Derecho de Cancelación o eliminación.

Corresponde a la facultad de todo titular de datos para exigir la destrucción de los datos almacenados, cualquiera fuere el procedimiento empleado para ello, cuando el almacenamiento de los datos carezca de fundamento legal o cuando estuvieren caducos. El dato carecerá de fundamento legal cada vez que se efectúe un tratamiento de datos en contravención de lo estatuido en la ley, por ejemplo, si se deroga la ley que lo autoriza.(Jervis Ortiz, 2002, p. 24). El dato puede devenir en caduco cuando: la ley así lo disponga, por el cumplimiento de la condición señalada para su vigencia, por la llegada del plazo señalado para su vigencia o bien, cuando se ha producido un cambio en las circunstancias o hechos que consigna, a menos que una norma expresa establezca lo contrario.

5.4.- Derecho de Oposición.

Es el que le corresponde a todo titular de datos para exigir la suspensión temporal de cualquiera de las operaciones del tratamiento de datos, este bloqueo procederá en todos aquellos casos en que la exactitud de los datos no pueda ser establecida o su vigencia sea dudosa y respecto de los cuales no corresponda la cancelación.

Si bien la ley define el bloqueo de datos como la supresión temporal de cualquiera de las operaciones del tratamiento de datos, lo cierto es que, en la práctica, el bloqueo de datos se traduce en la imposibilidad de comunicar el dato bloqueado a terceros. (Jervis Ortiz, 2002, pp. 24 - 25)

Estos derechos (acceso, rectificación, cancelación y oposición), denominados ARCO por la doctrina, son irrenunciables y el legislador se encarga de consignar que ellos no pueden ser limitados por medio de ningún acto o convención. Sin embargo, ello no impide que sea la propia ley la que establezca cuatro hipótesis donde se limita el ejercicio de estos derecho; las que se encuentran en el artículo 15 de la Ley 19.628:(Jervis Ortiz, 2002, p. 25)

a) Cuando impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido.
b) Afecte el derecho de reserva o secreto establecido en disposiciones legales o reglamentarias.
c) Afectación de la seguridad de la nación o el interés nacional. En este caso, se trata de conceptos jurídicos indeterminados por lo que será el juez, quien determine en definitiva si se dieron los presupuestos de hecho necesarios para considerar que la solicitud en cuestión por parte del titular de los datos pudo haber afectado la seguridad de la nación o el interés nacional.
d) Datos almacenados por mandato legal, salvo que la propia ley lo autorice.

6.- Habeas Data.

Esta garantía esencial de toda ley de protección de datos y las facultades que de ella derivan, están reguladas en los artículos 12, 13, 14 y 15 de la Ley 19.628, que son los primeros artículos del título II sobre "Derechos de los titulares de datos" y se ejercen precisamente ante quien aparezca como responsable del registro. (Jijena, 2001, p. 9)

La acción de habeas data representa una adecuación del tradicional *habeas corpus* a la protección de datos personales. Se trata de proveer un medio coercitivo para que la persona pueda acceder al reporte de sus datos personales, que son objeto de tratamiento de datos de terceros, cuando el requerido no se pronuncia de manera oportuna frente a su requerimiento, o responde con una negativa injustificada. (Donoso, 2013, p. 104)

Otros mecanismos que han sido utilizado por los titulares de datos para proteger sus derechos, han sido la interposición de acciones jurisdiccionales, tales como el recurso de protección, invocando como vulnerados el derecho a la honra, a la vida privada y el

derecho de propiedad. Con menor frecuencia, también se han interpuesto recursos de amparo económico, fundamentados en la vulneración de la garantía constitucional que asegura el libre desarrollo de la actividad económica; y demandas de indemnización de perjuicios por los daños causados por el tratamiento indebido de los datos.

Respecto a las causales o presupuestos facticos de procedencia del habeas data; estos son dos, el no pronunciamiento dentro del plazo legal, que es de dos días hábiles y la denegación injustificada; donde la ley al respecto distingue entre negativas fundadas en la necesidad de protección del interés nacional o la seguridad de la nación o negativas que no esgrimen este fundamento, lo cual tendrá importancia para los efectos de la determinación del Tribunal competente y del procedimiento aplicable.

El legitimado para interponer el recurso es el afectado, esto es, el titular de datos que ha visto vulnerados sus derechos reconocidos en la ley, con el objeto de solicitar amparo de ellos al Tribunal. Luego, el legitimado pasivo de este reclamo es el responsable del banco de datos, ya sea un particular u organismo público.

CAPITULO III

CHILE Y LA INSTITUCIONALIDAD DE CONTROL

1.- Aspectos Generales.

Uno de los principales obstáculos para que la Comunidad Europea considere a nuestro país como uno de aquellos que cuenta con los niveles adecuados de protección de datos está vinculado con la institucionalidad de control. Los Estados deben prever autoridades de control que supervigilen el tratamiento de datos personales, los cuales deben tener la calidad de independientes y deben contar con las atribuciones suficientes para dotarlas de efectividad en su función de velar por un tratamiento adecuado, con pleno respeto a los titulares de datos personales.

Entre los aspectos más controvertidos de la ley 19.628, resalta su falta de regulación respecto a la institucionalidad de control, destacando el hecho de que la ley sólo prevé una especie de autoridad de control respecto de los organismos públicos. En efecto, la ley 19.628 en su artículo 22 inciso 1, prevé el registro de los bancos de datos públicos en el registro que debe llevar el Registro Civil, siendo este uno de los ejes del principio de control.

La ley 20.285 de transparencia y acceso a la información pública[17], en su artículo 33 letra m) dispone que corresponderá al Consejo de la Transparencia "velar por el adecuado cumplimiento de la Ley N° 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado".

Si bien, ambas leyes se aprobaron por los legisladores chilenos con casi una década de diferencia, la Ley 19.628 en 1999 y la Ley 20.285 de 2008, ambos cuerpos legales regulan el mismo objeto, es decir, la información. El primero cautela la información que concierne a personas naturales identificadas o identificables, desde una perspectiva que pretende garantizar que sus titulares sean quienes decidan sobre su uso. El ámbito del segundo, en

[17] Disponible en: http://bcn.cl/msg (Consultada diciembre 2013).

cambio, es la información que obra en poder de los órganos del Estado (básicamente la administración pública), con la óptica de favorecer su conocimiento por parte de la ciudadanía.

La protección de los datos personales resguarda la intimidad y la autodeterminación informativa; la transparencia administrativa, en cambio, favorece la probidad y potencia la participación ciudadana. Todos ellos son bienes jurídicos reconocidos por nuestra Constitución y potencialmente, antagónicos. En efecto, parte de la información que obra en poder de los órganos públicos está constituida por datos personales. El conflicto entonces, es inevitable por lo que es necesario determinar a quién le encargaremos resolver este conflicto y se requiere hablar de una institucionalidad o de un órgano de control propiamente tal. (Rajevic, 2011, p. 139)

2.- Rol del Consejo para la Transparencia en materia de protección de datos.

El rol del Consejo para la Transparencia en protección de datos se desarrolla en tres ámbitos claramente definidos: la dictación de instrucciones en materia de transparencia, la resolución de casos, y la dictación de recomendaciones específicas. (Matus, 2010, pp. 6 - 10)

En materia de instructivos encontramos la instrucción General Número 4, sobre Transparencia Activa, que dispuso en lo relativo a datos personales lo siguiente:

a) Frente a los actos y resoluciones que tengan efectos sobre terceros, deben abstenerse de publicar datos personales que tengan carácter reservado conforme a lo establecido en los artículos, 10, 20 y siguientes de la Ley N° 19.628.
Asimismo, cuando se trate de actos administrativos sancionatorios, conforme al artículo 21 de dicha normativa, deben abstenerse de publicar los datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena y aplicarán, de ser procedente, el principio de divisibilidad respecto de los actos o resoluciones que los contengan.

b) Respecto al diseño, montos asignados y criterio de acceso a los programas de subsidios y otros beneficios que entregue el respectivo órgano, además de las nóminas de beneficiarios de los programas sociales en ejecución.

c) En la publicación de nóminas de beneficiarios de programas sociales en ejecución debe indicarse el nombre completo de los beneficiarios, la fecha de otorgamiento del beneficio y la identificación del acto por el cual se le otorgó, excluyendo determinados datos como, por ejemplo, domicilio, teléfono y correo electrónico del beneficiario, por no ser estrictamente necesarios para individualizarlo.

Mediante la Instrucción General N° 10, sobre el Procedimiento Administrativo de Acceso a la Información, se dispone:

a) En materia de formatos de presentación y requisitos de las solicitudes de acceso a la información, la identificación del solicitante exige la acreditación de la representación del requirente cuando se soliciten datos personales de la persona representada. Dicho poder debe constar en escritura pública o documento privado suscrito ante notario.

b) En cuanto a la prohibición de exigir el cumplimiento de requisitos en la solicitud no contemplados en la Ley de Transparencia ni en su Reglamento, los órganos deben abstenerse de requerir en los formularios de solicitud o en las solicitudes de acceso, como campo obligatorio, para efectos de registrarse en el sistema electrónico de solicitudes, permitir la presentación de las mismas o dar curso a una solicitud de acceso como requisito de admisibilidad, datos como número de cédula de identidad y/o rol único tributario, teléfono fijo o móvil, género o sexo, nivel educacional, estado civil y pertenencia a alguna institución.

c) En cuanto al análisis de la eventual afectación de derechos de terceros, procedimiento de notificación y ejercicio del derecho de oposición, la instrucción dispone que tratándose de datos sensibles en ausencia de oposición se entenderá que el tercero no accede a la

publicidad, debiendo aplicar el órgano público, de ser procedente, el principio de divisibilidad respecto de los documentos que los contenga.

d) Respecto de la revisión de la información y redacción de la respuesta, se considera como buena práctica que los órganos publiquen en Transparencia Activa, los actos administrativos por los cuales se acceda a las solicitudes de acceso a la información.

e) En materia de entrega efectiva de la información solicitada, señala que no se podrá condicionar la entrega a que el solicitante otorgue su autorización para el tratamiento de sus datos personales con finalidades distintas a las de efectuar la tramitación del procedimiento administrativo de acceso a la información, como puede ser el envío de un boletín informativo del servicio.

f) Cuando la información solicitada contenga datos sensibles de un tercero y se haya procedido a notificarlo, sin manifestarse consentimiento expreso por su parte, el órgano tachará aquellos datos en virtud del principio de divisibilidad, debiendo consignar en el formato respectivo que ello se debe a la aplicación de la Ley N° 19.628, y entregará la restante información.

En materia de recomendaciones; tratándose de resolución de casos, éste resulta ser el rol más interesante del Consejo para la Transparencia a la hora de valorar y ponderar ambos derechos en juego, dado que muchas veces las solicitudes de información recaen sobre documentos o antecedentes que contienen datos personales de terceros. El principio de máxima divulgación contenido en la normativa y el de finalidad de los datos personales ha tornado difícil el equilibrio de ambos derechos.

3.- Proyectos de Ley presentados desde el año 2005 y el Boletín N° 8143-03.

Los proyectos de ley enunciados a continuación representan algunas de las iniciativas de reforma legal vinculadas al tema analizado, y que tienen directa relación con la proposición de creación o establecimiento de una autoridad de control y que han sido presentados desde el año 2005, para discusión en el Congreso.

Boletín N° 3796 – 07. Año 2005.

- El proyecto se encuentra archivado sin discusión en sala.
- Modifica la ley N° 19.628 de protección de la vida privada, con el fin de evitar el uso abusivo de datos personales o de empresas y de resguardar a los usuarios de correos electrónicos de la propaganda comercial no solicitada.
- La propuesta cuenta con una ampliación en el ámbito de aplicación de la ley, extendiéndolo a las personas jurídicas; y con una modificación en la definición de "dato sensible" y "fuentes accesibles al público" entre otras.
- En el proyecto se manifiesta que, en relación a la autoridad de control; "La Ley chilena N°19.628 establece que en esencia, existen datos personales o nominativos que le pertenecen a sus titulares y que son "tratados" manual o automatizadamente, tanto por órganos públicos como por empresas o personas particulares, a quienes la ley califica como "responsables del registro o banco de datos". La regla general formalmente declarada por el texto legal es que dicho "tratamiento de datos personales" sólo puede hacerse en virtud de autorización legal o del titular de los datos, pero del contexto de las normas se desprende que la mayoría de los datos provienen de "fuentes de acceso público" (por lo cual no se requiere de autorización para su tratamiento) y se consagran importantes y amplias excepciones sobre todo en materia de datos "personales-patrimoniales", lo cual transforma a la regla general en una mera declaración de principios. El mecanismo de resguardo recogido parcialmente del Derecho Comparado se denomina "Derecho de Acceso" o "Habeas Data", y éste, después de ejercerse ante quien aparezca como responsable del banco de datos -si es que se tiene la suerte de ubicársele porque generalmente actúan en el anonimato- sólo puede reclamarse ante los tribunales ordinarios de justicia y no ante una autoridad administrativa."

Boletín N° 6120-07. Año 2008.

- El proyecto se encuentra en la etapa de primer trámite constitucional.
- Modifica la Ley 19.628 sobre protección de la vida privada y la ley N° 20.285 sobre acceso a la información pública.

- La propuesta incluye el reconocimiento explícito de derechos, la ampliación del margen de sujetos protegidos, el establecimiento de una autoridad de control, la distinción entre "encargado" y "responsable" de la base de datos, el fortalecimiento de los derechos de información, la regulación del flujo transfronterizo de datos, el aumento en las condiciones de seguridad en el tratamiento de datos, el reforzamiento del deber de rectificación y corrección de datos, la regulación de infracciones y sanciones, el perfeccionamiento del sistema de responsabilidad civil y la creación de un registro de bases de datos.
- Se destaca en el proyecto que "se requiere de una autoridad dotada de competencias y herramientas eficaces, tanto para dictar normativa sobre la materia, fiscalizar, adoptar medidas de resguardo y, en última instancia, sancionar los incumplimientos." Se manifiesta también que "La ley N° 19.628 no contempló un organismo administrativo, agencia o superintendencia estatal que se encargara de velar por el cumplimiento de sus normas, limitándose a entregar al Registro Civil e Identificación, el deber de llevar un registro de las bases de datos a cargo de organismos públicos. Ello ha hecho que en la práctica sea imposible fiscalizar el cumplimiento de las normas de la ley, y muchas de sus disposiciones se han tornado fútiles". A la vez, en el proyecto se deja constancia que "Considerando la necesidad de dar respuesta a las exigencias de protección del derecho a la autodeterminación informativa, sumado a la conciencia de que el establecimiento de una autoridad de control es fundamental para el real cumplimiento de la ley, se planteó la necesidad de incorporar facultades en esta dirección dentro de las competencias del Consejo para la Transparencia, durante la discusión parlamentaria de la ley N° 20.285. Sin embargo, sólo se incorporó la facultad de "Velar por el adecuado cumplimiento de la ley Nº 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado". Se tuvo conciencia de que ello sería insuficiente para el resguardo del tratamiento de los datos personales y los derechos de los titulares. Pero se concordó en avanzar y profundizar la actual regulación."
- El proyecto establece que la autoridad encargada de velar por el cumplimiento de la normativa, tanto la contenida en esta ley, como en otros cuerpos normativos, será el Consejo para la transparencia, creado por la ley N° 20.285. Por ello, dicho Consejo pasa ahora a denominarse "Consejo para la Transparencia y protección de datos personales".

Boletín N° 6495-07. Año 2009.

- Archivado sin discusión en sala.
- Modifica el artículo 19 N°4 de la Constitución Política, con el objeto de consagrar la protección y resguardo de los datos personales agregando los siguientes incisos segundo y tercero:

"Toda persona tiene derecho a controlar la información que le concierne, de modo de obtener un adecuado resguardo a sus derechos fundamentales.

"En ejercicio de este derecho, toda persona podrá conocer sus datos personales y los que le afecten personalmente o a su familia, y obtener su rectificación, complementación y su cancelación, si estos fueren erróneos o afectaren sus derechos constitucionales, de acuerdo con las regulaciones establecidas por la ley".

- En el proyecto se destaca: "Este derecho a la protección de datos personales se define como Habeas Data. Humberto Nogueira Alcalá define el Habeas Data como un derecho que asiste a toda persona a solicitar administrativamente y judicialmente la exhibición de registros o bases de datos -públicos o privados- en los cuales estén incluidos los datos personales o de su familia, para tomar conocimiento de su exactitud, solicitar su rectificación, superación, complementarlos o solicitar su reserva. Este derecho está recogido o reconocido por gran parte de las naciones europeas y americanas, por la Asamblea de las Naciones Unidas, así como por el Consejo de Europa.

Boletín 6594-07. Año 2009.

- El proyecto se encuentra en primer trámite constitucional.
- Reforma constitucional que crea una Agencia de Protección de Datos Personales.
- Incorpora en el artículo 19, numeral 4 de la Constitución Política de la Republica, a continuación de la expresión "familia" un punto seguido y la oración "Habrá una Agencia, autónoma y con personalidad jurídica, encargada de velar por la adecuada protección de los datos de carácter personal, resguardar la aplicación de las leyes y los derechos de los ciudadanos en la materia y los responsables de los registros privados o públicos.
- Se destaca en el proyecto: "Que entre las principales falencias sobre el particular (Ley 19.628); se señalan la inexistencia de registros respecto de las bases de datos particulares

existentes; las débiles sanciones para las infracciones a la ley, pues sólo se dispone de un proceso indemnizatorio en que deben acreditarse los perjuicios y las dificultades para frenar el uso indiscriminado de publicidad indeseada, por los más diversos medios, entre otros.

Que sin embargo, la mayor carencia es la inexistencia de un organismo público regulador de esta materia capaz de concentrar las funciones de registro y control de las bases de datos, resguardar los derechos de las personas y velar por la aplicación de la ley. Ello, en nuestra legislación se logra sólo supletoriamente a través del SERNAC cuando media una relación comercial entre las partes o de algunas Superintendencias, según la naturaleza de los datos involucrados, pero se carece de una instancia especializada, como ocurre, en otros, con los siguientes países y entidades de todo el orbe; como la Agencia Española de Protección de Datos (España), Comisión Nacional de la Informativa y de las Libertades (Francia), Comisionado Federal para la Protección de Datos (Alemania). Comisionado de Privacidad de Nueva Zelanda, entre otros.

Que resulta indispensable llenar esta carencia procurando la creación de un organismo público que asuma, a lo menos, las siguientes funciones:

a) Supervigilar a las entidades privadas y públicas que administren bases de datos,

b) Resolver administrativamente litigios entre los particulares y los administradores de los registros.

c) Informar a los ciudadanos respecto de sus derechos en materia de protección de datos personales.

Boletín 8143-03. Año 2012.

- El proyecto se encuentra en primer trámite constitucional.
- Los objetivos específicos del proyecto que se pueden destacar son el reforzamiento de los derechos de los titulares de datos personales; cumplir con los compromisos adquiridos por Chile en virtud de su incorporación a la OCDE, e incrementar los estándares legales de Chile para transformarlo en un país con un nivel adecuado de protección o "puerto seguro para el flujo de datos."
- Favorecer el desarrollo del mercado de los servicios globales en Chile como país receptor de dichas inversiones.

- A la vez, conforme a la descripción del proyecto este persigue: Precisar el objeto de protección de la Ley N° 19.628, a través de un nuevo artículo 1°, el que precisa el objeto de la Ley N° 19.628, enfatizando que corresponde a la protección de los datos personales, cualquiera sea el tipo de soporte en que consten, que permita su tratamiento por entidades privadas o públicas, vinculando dicha protección con el legítimo ejercicio del derecho de protección a la vida privada, garantizado a todas las personas en el número 4 del artículo 19 de la Constitución Política de la Republica.

Introduce el concepto de consentimiento previo, a través de un nuevo literal que define lo que debe entenderse por "consentimiento del titular", con el objeto de enmarcar que la licitud de todo tratamiento de datos personales requiere la manifestación expresa de voluntad de su titular, la cual debe efectuarse de manera libre, inequívoca e informada para que resulte valida.

Reforzamiento del Derecho a la Información por parte de los Titulares de Datos Personales y Definición de las Obligaciones del Responsable del Registro Base de Datos y del Encargado de todo o parte del Tratamiento de Datos Personales.

Establecimiento de la obligación de informar en comunicaciones comerciales y publicitarias el origen de los datos que permitieron su envío al titular y el derecho para este último de excluirse de la recepción de tales comunicaciones.

Establecimiento de procedimientos de reclamo más expeditos y equilibrados para los titulares de datos respecto de los responsables y encargados del tratamiento.

Creación de un catálogo de infracciones y de sanciones, el proyecto establece un catálogo pormenorizado de sanciones, en tres niveles, distinguiendo entre sanciones leves, graves y gravísimas, con sus respectivas sanciones, consistentes en multas y, en ciertos casos, cancelación del registro.

- Relacionado con la autoridad de control a modo de proposición se manifiesta el rol del SERNAC, al cual se le entregan atribuciones para informar, promover y proteger los derechos de los ciudadanos respecto a sus datos personales permitiéndole además presentar demandas colectivas. Pablo Longueira, Ministro de Economía, Fomento y Turismo, señala que "la autoridad encargada de la protección de datos personales en el ámbito privado es el SERNAC, ya que posee los recursos, el personal y la experiencia en esta materia". Lucas

del Villar, subdirector, del Servicio Nacional del Consumidor (SERNAC), sustenta las palabras anteriores, manifestando que "el Servicio Nacional del Consumidor (SERNAC), como institución encargada de velar por la protección de los derechos de los consumidores, constituye una instancia óptima para el adecuado resguardo de los derechos de los titulares de datos personales. Asimismo, destaca que el SERNAC ha abordado con anterioridad materias relativas a la protección de datos personales de los consumidores, desde una arista ligada a la responsabilidad precontractual y contractual que recae sobre los proveedores de productos y servicios: desde luego, el principio de buena fe obliga a los proveedores a actuar con lealtad respecto a los datos de carácter personal que son recopilados de los consumidores, sea antes de que la relación de consumo se concrete o en razón del perfeccionamiento de una determinada transacción comercial.

Teniendo especialmente presente la labor primordial del Servicio -educar, informar y proteger a los consumidores a través de las herramientas que le entrega la Ley del Consumidor-, la experiencia del SERNAC en el tratamiento y efectiva solución de los distintos conflictos que pueden derivarse de una relación de consumo, así como los crecientes niveles de eficacia y celeridad en la gestión de los asuntos de su competencia, constituyen un activo que repercutirá en la mejor protección de los derechos que asisten a los titulares de datos personales."

Eduardo Escalona, del Estudio Jurídico Escalona & Phillippi manifiesta que respecto al rol del Servicio Nacional del Consumidor en relación con la protección de datos personales de los ciudadanos, a su juicio es un organismo reconocido, con oficinas a nivel nacional, regional, provincial y con convenios que permiten cubrir casi todas las comunas del país. A la vez, manifiesta que "es mejor dotarlo de más recursos y personal, para cumplir con este tipo de funciones, antes que innovar con una nueva institución que quizás no cumplirá con estos requerimientos y que además tendrá domicilio solamente en Santiago o a lo más en las capitales regionales". El SERNAC señala, "puede ejercer todas las atribuciones que tiene disponibles para proteger a los consumidores respecto de datos personales y hoy en día en cumplimiento de su propia labor, ya supervisa algunas materias que dicen relación con datos personales particularmente respecto de los spam o comunicaciones indebidas o indeseadas a través de medios electrónicos". Advierte que la ventaja de adicionarle

atribuciones al SERNAC es que "contará directamente con la atribución de llevar registro electrónico de exclusión de las comunicaciones publicitarias y comerciales, es decir, estará directamente vinculado con aquello que dice relación con los intereses de los consumidores y además podrá promover acuerdos reparatorios. Por otro lado, se la dota de más recursos y personal, recursos que son equivalente a la reforma de SERNAC financiero, y además cuenta con ministros de fe que pueden levantar actas y certificar la infracción de esta ley."

La opinión contraria es manifestada por Claudio Ortiz, gerente general del Comité Retail Financiero, quien a su juicio "el proyecto no soluciona adecuadamente la orgánica y la falta de institucionalidad para asegurar el correcto cumplimiento de la normativa. La designación, no de uno, sino que de dos organismos a cargo de resolver las controversias y supervisión (SERNAC para el sector privado y Consejo de Transparencia para el sector público), está lejos de garantizar un mejor resguardo de los datos personales, creando disputas de autoridad y alejándose de las recomendaciones y exigencias dadas por la Unión Europea, con lo cual la reforma en los términos en que se encuentra propuesta no permitirá satisfacer las exigencias internacionales que nos permitan ser calificados como un país seguro en lo que se refiere a tratamiento de datos personales. Por lo que la idea es implementar el modelo de los países desarrollados mediante la creación de un órgano especializado; una Autoridad de Protección de Datos o equivalente, autónomo, con un ámbito de gestión tanto en el sector público como privado, que cumpla las como sus funciones básicas, la promoción de los Derechos de las personas respecto de sus datos y labores educativas; promoción de acuerdos de autorregulación con las empresas que tratan datos personales, monitoreo permanente de la realidad internacional y promoción de acuerdos bilaterales para el tránsito trasfronterizo de los datos, entre otros.

Daniel Álvarez, profesor de la Facultad de Derecho de la Universidad de Chile, manifiesta que respecto de la autoridad de control, "las propuestas que están el proyecto son insuficientes, ya que la distinción entre tratamiento de datos que realizan organismos públicos y los organismos privados en muchos casos es irrelevante, toda vez que toda la información personal de los teléfonos, por ejemplo no pasa por ningún organismo público. Por lo tanto, hoy día no hay ningún organismo público con facultades de aplicar sanción ni compeler a las empresas de telecomunicaciones para que hagan un trato adecuado de datos

personales. Indica que en la práctica las empresas lo hacen, por lo que hay un buen estándar de facto de protección, ya que han sido conscientes de que estamos ante un problema de garantías constitucionales, y si hay afectación grave de derechos, es constitutiva de delito." A su juicio, "si se va a establecer una autoridad de control, esta debiera tener potestad sobre el mundo público y sobre el privado, ya que en su opinión no tiene sentido hacer esta distinción."

Respecto al SERNAC, señala que "en la actualidad no tiene facultades para aplicar sanciones, por lo que los afectados necesariamente tienen que ir a Tribunales, lo cual no ocurre en la práctica, por lo que judicializar la protección de datos personales ha quedado demostrado desde el año 1999 a la fecha, es ineficiente. En consecuencia, la autoridad que se establezca tiene que tener competencia para al mundo público como el privado y, además, tiene que tener facultades sancionadoras. Recomendó agregarle al Consejo para la Transparencia la facultad de control en el ámbito privado, y así solo en casos de alta complejidad se podría recurrir a los Tribunales de Justicia."

Finalmente Renato Jijena, profesor de derecho informático de la Pontificia Universidad Católica de Valparaíso, expresa como uno de los aspecto negativo del proyecto el que se pretenda subsanar la inexistencia de un órgano fiscalizador o Autoridad de Control, asignando competencia al efecto al SERNAC en el sector privado y al Consejo de Transparencia en el sector público, sin conferir las competencias y herramientas necesarias a una autoridad autónoma para velar por el adecuado cumplimiento de las normas sobre protección de datos. A la vez, señala que "la ley 19.628 posee una parte dogmática débil, no tiene parte orgánica, no contempla procedimientos administrativos de tutela sino uno judicial y engorroso, y no posee un arsenal sancionatorio adecuado. Chile sería, de aprobarse esta idea de legislar, el único país del mundo donde la función de Autoridad de Control y Protección de Datos se dividiría entre dos entes persé no idóneos."

CAPITULO IV

MECANISMOS DE CONTROL EN LA LEGISLACIÓN EXTRANJERA SOBRE EL TRATAMIENTO DE DATOS PERSONALES.

Alemania.

- Tipo de Autoridad.

El comisionado Federal para la Protección de Datos (*Bunderbeauftragter Fur den Datenschutz*), creado por la Ley de Protección de Datos alemana tiene la función de velar por el cumplimiento de la ley en el sector público, y es nombrado por el Presidente de la Federación tras haber sido elegido por el Bundestag.

Junto al Comisionado se han creado otras dos figuras, el Oficial para la protección de datos (*Beaufragter fur den Datenschutz*) y la Autoridad de Supervisión (*Aufsichtsbehorde*). El Oficial es nombrado por cada organismo, público o privado, que desee realizar un tratamiento de datos personales y la Autoridad de Supervisión, puede ser designada por los Gobiernos de los *Lander*.

- Atribuciones

El Oficial tiene como tarea "vigilar" los tratamientos de datos que el mencionado organismo realice.

La Autoridad de Supervisión, se encarga de comprobar todos los tratamientos de datos personales que se realicen, llevando un registro de los mismos y pudiendo notificar las infracciones que se cometan a los órganos competentes en función de la infracción cometida.(Arenas, 2005, p. 7)

- Mecanismos

En Alemania, la ley de protección datos de 1977 contemplaba algunos tipos penales e infracciones asociados al tratamiento de datos, los primeros sancionados inclusive con penas privativas de libertad, los segundos con multas de monto variable. Entre estos últimos, a efectos de resguardar la vigencia de los propios medios de control contemplados

en la ley, se sanciona la omisión y extemporánea designación de comisario de protección de datos o notificación de inicio de actividades de procesamiento de datos, y obstaculizar las labores de fiscalización de la autoridad de tutela estatal. Mientras, la nueva Ley de Protección de Datos de 1990 abundó en la tipificación de los ilícitos penales e infraccionales asociados al tratamiento de datos. (Cerda, 2006, p. 233)

Argentina

- Tipo de Autoridad.

El artículo 1 de la ley 25.326 señala que la misma tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre. El órgano de control es la Dirección Nacional de Protección de Datos Personales, que funciona en el ámbito de la Secretaria de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos.

- Atribuciones.

El órgano de control debe realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la ley; es por eso, que podemos destacar las siguientes funciones:

- Asistir y asesorar a las personas que lo requieran acerca de los alcances de la ley.
- Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por la ley.
- Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos.
- Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o banco de datos. A tal efecto puede solicitar autorización judicial para acceder a locales, equipos o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la ley.

- Solicitar información a las entidades públicas y privadas.
- Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la ley.
- Constituirse en querellante en las acciones penales que se promovieran por violaciones a la ley.

- Mecanismos

Los ciudadanos pueden ejercer las siguientes acciones en caso de incumplimiento de la ley (Ministerio de Justicia y Derechos Humanos; Presidencia de la nación, 2013):

- Supresión de datos personales de registros de bases de datos en caso de comprobarse el hecho denunciado.
- Rectificación de datos personales de registros de bases de datos.
- Acceso a la Información.
- Actualización de datos personales.
- Confidencialidad en el tratamiento de datos.

Además se cuenta con procedimientos de inspección, los que tienen por objetivo:

- Tomar conocimiento de las actividades del responsable de la base de datos, los datos personales que administra, y los medios y la forma con los que lo hace.
- Evaluar el grado de cumplimiento lo prescrito por la Ley N° 25.326.
- Realizar recomendaciones para el mejor desempeño del responsable dentro del marco legal.

Dinamarca

- Tipo de Autoridad.

La ley sobre tratamiento de datos personales, se encuentra bajo la Autoridad de la Agencia de Protección de Datos Danesa, la que consta de un Consejo y una Secretaría. Se trata de un órgano independiente, que ejerce sus funciones libres de órdenes e instrucciones. (Arenas, 2005, p. 15)

- Atribuciones

La Agencia Danesa de Protección de Datos está encargada de la supervisión de todos los tratamientos de datos personales que entren en el campo de apelación de la normativa danesa.

Este deber se lleva a cabo, en parte, al proporcionar orientaciones y asesorar a las autoridades, las empresas y los ciudadanos.

A través de notificaciones y autorizaciones,la Agencia Danesa de Protección de Datos puede controlar algunos de los procesamientos más sensibles de los datos personales que se llevan a cabo por las autoridades y empresas.

En caso de quejas de los ciudadanos, la Agencia Danesa de Protección de Datos puede tomar decisiones acerca de si determinadas operaciones de transferencia están en conformidad con la Ley de Tratamiento de Datos de Carácter Personal.

La Agencia Danesa de Protección de Datos lleva a cabo una serie anual de inspecciones de las autoridades públicas y las empresas privadas que han recibido la autorización de la Agencia para tratar datos personales, inspeccionando si el tratamiento de datos se lleva a cabo en conformidad con la Ley sobre tratamiento de Datos Personales. (Datatilsynet, 2013)

- Mecanismos.

Si la Agencia Danesa de Protección de Datos descubre violaciones punibles de la Ley sobre Tratamiento de Datos personales en relación con el manejo de una queja o una inspección, está autorizada para emitir un aviso de prohibición o de ejecución o incluso, reportar la violación a la policía. (Datatilsynet, 2013)

España.

- Tipo de Autoridad.

En el título VI de la Ley Orgánica 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal, se regula la Agencia de Protección de Datos, la que es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que

actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se rige por lo dispuesto en la Ley y en un Estatuto propio, que fue aprobado por el Gobierno. (AGPD, 2013)

- Atribuciones

Son funciones de la Agencia de Protección de Datos: (AGPD, 2013)

- Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
- Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.
- Atender las peticiones y reclamaciones formuladas por las personas afectadas.
- Requerir a los responsables y los encargados de los tratamientos la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.
- Ejercer la potestad sancionadora.
- Redactar una memoria anual y remitirla al Ministerio de Justicia.
- Informar acerca de los derechos reconocidos en la Ley
- Promover campañas de difusión a través de los medios.
- Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente.

- Mecanismos

En cuanto al procedimiento para la tutela de los derechos, el artículo 18 establece que las actuaciones contrarias a lo dispuesto en la presente ley pueden ser objeto de reclamación

por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

Puede el interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma[18], que deberá asegurarse de la procedencia o improcedencia de la denegación. La ley dispone también que contra las resoluciones de la Agencia de Protección de Datos proceda recurso contencioso – administrativo.

En cuanto a las sanciones, la ley contempla una escala de multas que varía dependiendo de la gravedad de la infracción cometida por el responsable de los ficheros donde se encuentre la información, según lo disponen los artículos 44 y 45 de esta. (Castro Martines, Karla. Moreno Carrasco, Diego, 2012, pp. 485 - 486)

Finlandia

- Tipo de Autoridad.

El Defensor del Pueblo, es una autoridad del Estado encargada de garantizar los derechos de los ciudadanos ante abusos que puedan cometer los poderes ejecutivos y, en su caso, legislativo de ese mismo Estado, ateniendo denuncias de persona a instituciones, organismos, etc.

En el ámbito de los datos personales existe el Defensor del Pueblo de Protección de Datos y la Oficina del Defensor del Pueblo de Protección de Datos.

- Atribuciones

La Constitución de Finlandia garantiza la vida privada de todos los ciudadanos, la honra, la inviolabilidad del domicilio. La protección de los datos personales se estipula en detalle por la ley correspondiente. Uno de los objetivos de la Ley de Datos personales es el de mejorar la oportunidad de las personas para controlar el uso de sus datos personales. Las personas

[18]Existen tres Agencias Autonómicas de Protección de datos en España; 1) Agencia de Protección de Datos en la Comunidad de Madrid. 2) Autoridad Catalana de Protección de Datos y 3) Agencia Vasca de Protección de Datos.

tienen el Derecho de saber por qué y cómo los datos personales están siendo procesados y decidir sobre el tratamiento, a menos que se estipule lo contrario en la ley.

El Defensor del Pueblo de Protección de Datos y la Oficina del Defensor del Pueblo de Protección de Datos proporcionan orientación y asesoramiento sobre todas las cuestiones relacionadas con el tratamiento de datos personales y controlan el cumplimiento de la ley de Datos Personales. (DataOmbudsmannensByra, 2013)

Los objetivos de la Oficina del Defensor del Pueblo son:

- Mantener y promover el derecho a la intimidad.
- Cooperar con los interesados y los controladores y las organizaciones que los representan, así como otros organismos relacionados, con miras a la prevención de la violación de la privacidad.
- Promover el desarrollo y el cumplimiento de las buenas prácticas de procesamiento de datos.
- Asistencia y apoyo al desarrollo y uso de sistemas de apoyo y protección de la privacidad.

- Mecanismos

Los mecanismos son variados, pero gran parte de ellos recae en los deberes que debe realizar el Defensor del Pueblo de Protección de Datos, como por ejemplo, el ejercer el poder en cuestiones relacionadas con la aplicación del derecho de la verificación y la corrección de los datos personales. A la vez, la Ley de Datos Personales hace hincapié en el registro de mantenimiento; donde el Defensor del Pueblo de Protección de Datos proporciona orientación y consulta en la elaboración y revisión de los códigos de conducta. También, el Defensor del Pueblo de Protección de Datos, debe ser oído en materia de preparación de reformas legislativas o administrativas relativas a la protección de los derechos y libertades de las personas en el tratamiento de datos personales. En la práctica, esto significa que el Defensor del Pueblo ofrece declaraciones y participa en los grupos de trabajo creados para la elaboración y revisión de la legislación.

La supervisión se realiza a través de una obligación legal del controlador de la notificación, sin embargo, incluso en algunas excepciones pueden ser aceptados en el marco de la Directiva de Protección de Datos. Las inspecciones tienen por objeto evaluar el cumplimiento de datos, controladores de rectores, la mejora de la calidad de los sistemas y la prevención de violaciones de los Datos Personales.(DataOmbudsmannensByra, 2013)

México

- Tipo de Autoridad.

El Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), se encuentra definido en el artículo 33 de la Ley Federal de Transparencia y Acceso a la Información Pública gubernamental, como un órgano de la Administración Pública Federal, con autonomía operativa, presupuestaria y de decisión, encargado de promover y difundir el ejercicio del derecho de acceso a la información, resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de las dependencias y entidades.

Posteriormente con la dictación y publicación el año 2010 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), se ampliaron las facultades y atribuciones del Instituto, incluyéndose lo relativo a la fiscalización y tutela de la protección de datos personales. Además, con la dictación de esta ley, se modificó el nombre del Instituto, pasando a ser actualmente el Instituto Federal de Acceso a la Información y Protección de Datos, según lo dispone el artículo sexto transitorio. (IFAI, 2013)

- Atribuciones.

En cuanto a las atribuciones del Instituto en lo que respecta a la protección de datos encontramos:

- Vigilar y verificar el cumplimiento de las disposiciones contenidas en esta Ley, en el ámbito de su competencia, con las excepciones previstas por la legislación.
- Interpretar en el ámbito administrativo la Ley.
- Proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en la Ley.

- Emitir los criterios y recomendaciones, de conformidad con las disposiciones aplicables de esta Ley, para efectos de su funcionamiento y operación.
- Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos, las finalidades del tratamiento y las capacidades técnicas y económicas del responsable.
- Conocer y resolver los procedimientos de protección de derechos y de verificación señalados en la Ley e imponer las sanciones según corresponda.
- Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos.
- Rendir al Congreso de la Unión un informe anual de sus actividades.
- Acudir a fotos internacionales en el ámbito de la Ley.
- Elaborar estudios de impacto sobre la privacidad previos a la puesta en practica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes
- Desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales en Posesión de los particulares y brindar capacitación a los sujetos obligados.
- Las demás que le confiera la ley y demás ordenamientos aplicables.

- Mecanismos.

La Ley Federal de la protección de datos personales en posesión de particulares contempla un procedimiento específico en caso de que el titular del derecho de protección de datos personales se vea afectado, en el capítulo VII de esta ley, artículo 45 y siguientes. Además, el artículo 56 contempla la posibilidad de que las partes puedan promover juicio de nulidad contra las resoluciones del Instituto, ante el Tribunal Federal de Justicia Fiscal y Administrativa.

En cuanto a las sanciones, estas se encuentran reguladas en el Capítulo X, artículo 64 y consisten principalmente en multas, cuyo valor va a depender del tipo de infracción cometida y en apercibimiento para que el responsable del banco de datos lleve a cabo los actos solicitados por el titular. (IFAI, 2013)

Reino Unido

- Tipo de Autoridad.

La Oficina del Comisionado de Información (ICO) que es el órgano público independiente del Reino Unido

- Atribuciones

El ICO está establecido para fomentar el acceso a la información oficial y proteger la información personal. Lleva a cabo este cometido promocionando prácticas recomendables, dictaminando en quejas que reúnen las condiciones exigidas, proporcionando información a personas físicas y organizaciones y tomando las medidas adecuadas cuando se infringe la ley. (ICO, 2013)

Las funciones de ICO incluyen tratar asuntos de protección de datos para todo el Reino Unido y asuntos de libertad de información para Inglaterra, Irlanda del Norte y Gales. Las tres oficinas regionales, que fueron establecidas en 2003, responden ante los problemas locales y forjan relaciones con grupos de interés regional.

El objetivo general de ICO es conseguir:

- Hacer pública la información oficial a menos que existan buenas razones para no divulgarla.
- Asegurar que se proteja adecuadamente la información personal.

- Mecanismos

Existen una serie de herramientas a disposición de la Oficina del Comisionado de Información para la adopción de medidas y cambiar el comportamiento de las organizaciones y las personas que recogen, utilizan y mantienen la información personal.

Esto incluye desde la persecución penal, la aplicación de distintas medidas no penales como también, de auditoría. El comisionado de Información también tiene el poder para llevar a cabo una multa monetaria en el caso de los controladores de datos. (ICO, 2013)

Uruguay.

- Tipo de Autoridad.

La Unidad Reguladora y de Control de Datos Personales (URCDP). Se trata de un Órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). Fue creada por la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data (LPDP), con autonomía técnica, cuya competencia es custodiar el cumplimiento de la legislación de protección de datos personales y asegurar el respeto de sus principios. (URCDP, 2013)

- Atribuciones.

El órgano de control debe realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la ley:

- Asistir y asesorar a las personas que lo requieran acerca de los alcances de la ley y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza.
- Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por la ley.
- Realizar un censo de las bases de datos alcanzados por la ley y mantener el registro permanente de los mismos.
- Controlar la observancia de las normas sobre integridad, veracidad y seguridad de datos por parte de los responsables de las bases de datos, pudiendo a tales efectos realizar las actuaciones de inspección pertinentes.
- Solicitar información a las entidades públicas y privadas.
- Emitir opinión toda vez que le sea requerida por las autoridades competentes.
- Asesorar en forma necesaria al Poder Ejecutivo en la consideración de los proyectos de ley que refieran total o parcialmente a la protección de datos personales.
- Informar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables, en forma gratuita.

- Mecanismos.

En cuanto a los mecanismos, nos encontramos con la acción jurisdiccional de habeas data. Su legitimación y objeto, recaen en el titular al que se le niegue el acceso, rectificación, inclusión o supresión de datos en 5 hábiles o no se le justifique negativa.

Destaca también el proceso sumario, que corresponde a una audiencia pública en 3 días, en la que se produce prueba, alegatos y sentencia, ésta prorrogable por breve plazo, excepcionalmente hasta 3 días. La sentencia fija conducta a cumplir en plazo de hasta 15 días corridos; la apelación no suspende el amparo y el tribunal superior tiene 4 días para decidir.

CAPITULO V

CONCLUSIONES Y PROPUESTAS

CONCLUSIONES.

1) La protección de los datos personales como derecho fundamental, ha tenido un desarrollo constante, comenzando sus primeros pasos a través de la *"Privacy Norteamericana"*; mientras que el sistema europeo, se inicia con la construcción de la protección de datos a partir del derecho a la intimidad, del derecho al honor y a la propia imagen, los que fueron cobrando relevancia atendido el avance del desarrollo tecnológico.

2) En nuestro país, se contemplan diversas normas, tales como aquellas contenidas en la Constitución Política de la República, la Ley 19.628, Ley 20.285, entre otras, que regulan aspectos relativos a los archivos y gestión de documentos, generando una dispersión normativa que ocasiona grandes problemas al momento de aplicar e interpretar las disposiciones en concordancia con la realidad que hoy se puede observar.

3) La Constitución Política de la República de Chile, en su artículo 19 número 4, asegura a todas las personas el respeto y protección a la vida privada y pública y a la honra de la persona y de su familia.

4) Si hablamos de los bienes jurídicamente protegidos, el problema de fondo se origina por un conflicto entre el legítimo interés de aquellas personas cuyos datos nominativos se procesan computacionalmente, en resguardar su vida privada. Mientras que también hay un interés legítimo que poseen los gobiernos y los particulares para acceder a cierta información.

5) A nivel legal, en Chile la ley 19.628 de 1999, en términos generales, establece los principios y algunas estipulaciones necesarias para regular el mercado de tratamiento de datos. La ley 19.628; manifiesta lo que se entenderá por almacenamiento de datos, transmisión de datos, dato caduco, dato sensible, eliminación o cancelación de datos, modificación de datos, entre otros.

6) Conforme al ámbito de aplicación, el ámbito material, recae en aquel tratamiento de datos de carácter personal verificado en forma automatizada y manual. En cuanto al ámbito

subjetivo de aplicación, el titular de datos personales lo es sólo la persona natural a quien ellos se refieren y el responsable del registro o banco de datos.

7) Los principios relativos al tratamiento de datos, son 1) La libertad en el tratamiento de datos personales, 2) Información y consentimiento del titular, 3) Finalidad, 4) Calidad de los datos, 5) Desigualdad en el tratamiento de los datos personales, 6) Deber de secreto, 7) Temporalidad. Todos estos, tienen manifestaciones en la ley 19.628.

8) Los derechos de los titulares de datos son: 1) Derecho de información o Acceso, 2) Derecho de modificación, 3) Derecho de cancelación o eliminación y 4) Derecho de Oposición.

9) Entre las principales deficiencias de la ley encontramos que no propende a un equilibrio entre la información que poseen las instituciones privadas en el tratamiento de datos personales, ya que sólo existe un registro de datos públicos, el que ni siquiera es completo, lo que lleva a que los titulares de datos personales desconozcan quien trata su información personal y cómo lo hace. A la vez, no existe regulación respecto de la transferencia transfronteriza de datos, lo que hace que nuestro país no cumpla en esta parte con los estándares internacionales y se dificulte este tipo de transferencias, como así mismo, que nuevamente los titulares de la información que se transfiere, tengan poco o nada que decir al respecto.

10) Y quizá la más importante, es que la institucionalidad de Control en nuestro país solo es considerada para los organismos públicos, recayendo en un registro de los bancos de datos públicos que es llevado a cabo por el Registro Civil, Además la ley 20.285 de transparencia y acceso a la información pública en su artículo 33 letra m) dispone que otorga al Consejo para la Transparencia La dictación de instrucciones en materia de transparencia, la resolución de casos y la dictación de recomendaciones específicas. En este sentido, nuestro país no cuenta con una autoridad independiente que se encuentre permanentemente velando por el cumplimiento de la ley tanto por parte de los organismos públicos como privados, que tenga la posibilidad de aplicar sanciones por el incumplimiento y que tenga un fuerte rol de promoción de la protección de datos personales, siendo este uno de los vacíos que aparece como la mayor dificultad para que nuestro país pueda cumplir el estándar internacional exigido.

11) A partir de lo anterior, podemos concluir entonces que, en nuestro país, no existe un órgano de control independiente, lo que obliga a los particulares a recurrir a los Tribunales de Justicia como forma de poder proteger las distintas injusticias, a la vez, no existe un registro de bases de datos privadas, lo que dificulta claramente el ejercicio de los derechos especialmente a personas naturales.

12) Los mecanismos de control en la legislación comparada son variados, la Dirección Nacional de Protección de Datos Personales dentro del Ministerio de Justicia y Derechos Humanos en Argentina, en España la Agencia de Protección de datos, el Instituto Federal de Acceso a la Información y Protección de Datos en México.

PROPUESTAS.

Respecto a las propuestas, estas pueden concentrarse en cuatro específicamente:

1) La existencia de un solo procedimiento y la creación de una normativa específica sobre la materia de protección de datos personales que la considere como derecho autónomo y específico; lo que claramente permitiría la existencia de un solo cuerpo legal de datos personales facilitando el ejercicio del derecho, dejando de lado la dispersión normativa existente en nuestro país completando los vacíos legales y evitando la dificultad de poder lograr el integro conocimiento y comprensión de la estructura legal en esta materia.

2) El establecimiento de una autoridad de control independiente y de rango constitucional. Su existencia acarrea una serie de ventajas, ya que al tratarse de un órgano independiente, permite imparcialidad en el desempeño de sus funciones, eliminando potenciales conflictos de intereses que se generan cuando esta función queda bajo el alero de una autoridad dependiente de uno de los poderes sujetos al ámbito de la aplicación de la ley, o cuando la responsabilidad del ejercicio del derecho queda en manos del que realiza el tratamiento de los datos. Una autoridad independiente se encuentra en una mejor posición frente a la necesaria tarea de evaluar las fortalezas y debilidades de la ley de protección de datos personales que se mantenga vigente en un determinado país, de manera que pueda conducir a estudios y discusiones desde el campo de la sociedad civil, para mejorar los aspectos resueltos o que sean perfectibles en dicho cuerpo normativo.

Una entidad independiente, puede llevar a cabo una tarea que no ha sido objeto de análisis ni de medidas a tomar y a realizar, que es la creación de planes educativos y de capacitación en materia de ejercicio y de conocimiento de este derecho, para que exista un real aprovechamiento de su consagración a nivel normativo, colaborando en la existencia de condiciones que permitan el ejercicio de este derecho. Así mismo, se requiere que la ciudadanía tome conciencia del valor de sus datos personales y de las facultades que tiene sobre estos.

3) La autoridad de control, debe contar con poderes de investigación, de intervención y con capacidad procesal en caso de infracciones nacionales, tanto de las disposiciones comunitarias o para informar de éstas a la respectiva autoridad judicial. Además, si en el cumplimiento de sus funciones estas autoridades provocan la lesión de los derechos de los titulares de los datos, debe existir la posibilidad de interponer recursos jurisdiccionales contra ellos.

4) La creación de un registro público de base de datos privada, puesto que existe una gran cantidad de información que se maneja en este nivel y del cual no se tiene conocimiento ya que no se encuentra registrada. Para este efecto, es importante considerar y tener en cuenta que la mayoría de las bases de datos no se encuentran en poder del Estado, sino que se encuentran en manos del sector privado, tales como bancos, isapres, compañías de seguros, AFP, farmacias, clínicas, empresas de servicios tecnológicos, partidos políticos, condominios de edificios que exigen acreditación entre otros.

BIBLIOGRAFIA CONSULTADA

Agencia Española de Protección de Datos (2004): Guía del derecho fundamental a la protección de datos de carácter personal.pp.40. Disponible en http://www.agpd.es/portalwebAGPD/common/FOLLETO.pdf Fecha de última consulta; 24/Noviembre/2013.

Aguilar, García Nicolás (1998): "La cuestión de la responsabilidad en el derecho informático" *REDI Revista electrónica de derecho informático,* editorial vLex, número 2 septiembre 1998 pp.14

Anguita Ramírez, Pedro. (2007): *La protección de datos personales y el derecho a la vida privada: régimen jurídico, jurisprudencia y derecho comparado: análisis de la ley No. 19.628 sobre protección de la vida privada (protección de datos de carácter personal) modificada por la ley No. 19.812.* Santiago de Chile: Editorial Jurídica de Chile.

Arrieta, Raúl; Ortiz, Claudio: Uriarte, Mikel; Gutiérrez Rodrigo; Donoso, Lorena; Cordero, Luis (2009). "Chile y la protección de datos personales ¿Están en crisis nuestros derechos fundamentales?" Ediciones Universidad Diego Portales, Santiago, Chile. Disponible en http://www.expansiva.cl/media/publicaciones/libros/pdf/7.pdf Fecha de última consulta: 24/Noviembre/2013.

Barriuso Ruiz, Carlos. (2009): Las redes sociales y la protección de datos hoy. en *Anuario Facultad de Derecho*, Universidad de Alcalá II (2009) pp. 301- 338

Baum Erica (2000) "La propiedad de la información" en *REDI Revista Electrónica de Derecho informático,* editorial vLex, número 18, Enero 2000.

Bazan, Víctor (2005): "El habeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado" en *Estudios Constitucionales, Revista Semestral del Centro de Estudios Constitucionales.* Universidad de Talca, Chile, Año 3 Número 2Pp. 85 a 139.

BCN, Historia de la Ley Número 19.628 Protección de la Vida Privada. http://www.leychile.cl/Navegar/scripts/obtienearchivo?id=recursoslegales/10221.3/2468/7/HL19628.pdf Fecha de última consulta: 24/Noviembre/2013.

Bru, Cuadrada Elisenda 2007 "La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad." Septiembre. Revista de Internet, derecho y política. PP.15

Davara Rodríguez, Miguel Ángel. (1998): *La protección de datos en Europa: Principios, derechos y procedimiento.* Madrid, Grupo Asnef Equifax 1998.

Días, Arias Rafael. (2000) "España: Transferencia de Datos personales. ¿Llegaran nuestros datos a buen puerto?"en *REDI Revista Electrónica de Derecho Informático* Editorial vLex, Numero 23, junio 2000.

Cámara de Chile (Septiembre 2011), Asesoría Legal Ministerio de Economía, Fomento y Turismo: Comentarios Anteproyecto de ley de datos personales, ley 19.628. http://webcache.googleusercontent.com/search?q=cache:vo1nKvb9F2UJ:www.cnc.cl/downloadfile.aspx%3FCodSistema%3D20020129172812%26CodContenido%3D20121016181041%26CodArchivo%3D20121203115636+&cd=3&hl=es&ct=clnk&gl=cl Fecha de última consulta: 24/Noviembre/2013.

Donoso, Lorena, "El tratamiento de datos personales en el sector de la educación" en *En foco N°136,* Expansiva UDP. Disponible en: http://www.expansiva.cl/publicaciones/en_foco/detalle.tpl?iddocumento=15042009150219 Fecha de última consulta: 24/Noviembre/2013.

Celare (Agosto 2011), Revista de Relaciones Euro latinoamericanas: La protección de datos en la unión europea y América Latina.Nº83 – Año 17. http://www.celare-alcue.org/eurolat/euro83.pdf Fecha de última consulta: 24/Noviembre/2013.

Cerda, Silva Alberto. (2003) "Autodeterminación Informativa y leyes sobre protección de datos." en *Revista chilena de derecho informático. Centro de Estudios de Derecho Informático.* Universidad de Chile, Santiago, Chile. Disponible en:

http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/viewArticle/10661/11413 Fecha de última consulta: 24/Noviembre/2013.

Cerda, Silva, Alberto: (2011): "El nivel adecuado de protección para las transferencias internacionales de datos personales desde la unión europea", en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso,* Valparaíso, Chile, N° XXXVI, pp.327-356.

Errázuriz Amenábar, Sebastián. (2005): *Protección jurídica de datos personales. Ley numero 19.628* Santiago, Chile, 2005.

Chen, Mok, Susan (2010): Privacidad y protección de datos: Un Análisis de legislación comparada. En *Diálogos, Revista Electrónica de Historia,* ISSN: 1409-469X, Vol. 11 Nº1, febrero-agosto 2010, pp.111-152.

Fundación Pro Acceso (2008): Hacia una nueva institucionalidad de acceso a la información pública en Chile. Junio 2008. Pp.160. Disponible en: http://www.cdc.gob.cl/wp-content/uploads/documentos/nueva_institucionalidad_proacceso_junio_2008.pdf

García, González Aristeo (2007): "La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado". En *Boletín Mexicano de Derecho comparado* nueva serie año XI, número 120 Septiembre – Diciembre de 2007, pp. 743 – 778

García, Ninet. José Ignacio; Paches, Fernando de Vicente. *El derecho valor a la dignidad humana y el derecho a la protección de datos personales en la Constitución Europea*, Revista del ministerio de trabajo y asuntos sociales. Disponible en: http://webcache.googleusercontent.com/search?q=cache:i2fGISLn5goJ:www.unav.es/matrimonioyfamilia/b/uploads/24573_Garcia-Vicente_MTAS2005_Derecho.pdf+&cd=1&hl=es&ct=clnk&gl=cl Fecha de última consulta: 24/Noviembre/2013.

Gregorio, Carlos. Instituto de Investigación para la Justicia: Protección de datos personales en América Latina. Fecha de última consulta: 24/Noviembre/2013.

Herran, Ortiz, Ana Isabel. (2001) "La protección de datos personales en el marco de la Unión Europea" en *REDI Revista Electrónica de Derecho Informático.* Editorial vLex Numero 39, Octubre 2001.

Herrera Bravo, Rodolfo (2001) "Chile: ¿Por qué la protección de datos personales es una garantía básica de los derechos fundamentales?" en *REDI Revista electrónica de Derecho Informático.* Editorial vLex, Número 38, Septiembre 2001.

Hess, Araya, Christian (2002): Derecho a la Intimidad y Autodeterminación informativa, en: http://www.democraciadigital.org/derechos/arts/0201intimidad.html Fecha de última consulta: 24/Noviembre/2013

Jaña Tapia, Washington Alejandro. (2003) *Análisis legal comparativo de la protección de datos personales a nivel latinoamericano.* Santiago, Chile.

Jijena, Renato Javier. (1999): Sobre la no protección de la intimidad en Chile. Analisis de la ley 19.628 de agosto de 1999.en*REDI revista electrónica de derecho informático,* editorial vLex, número 39, octubre 2001. Pp.12

Jijena, Leiva, Renato: (2010): "Actualidad de la Protección de Datos Personales en América Latina, el Caso de Chile", en *Memorias del XIV Congreso Iberoamericano de Derecho e Informática*, Monterrey, México, pp. 413-431.

Jofré Vásquez, Andrea (2005): *La protección de datos de carácter personal y la importancia de una autoridad de control* Santiago, Chile.

Lara, Carlos Juan. Vera, Francisco y Soto, Bárbara (2005) "Privacidad y nuevas tecnologías, regulación chilena y propuestas de política pública" en *ONG Derechos Digitales*. Santiago, Chile. Disponible en: http://www.derechosdigitales.org/wp-content/uploads/pp-02.pdf. Fecha de última consulta: 24/Noviembre/2013.

López Román, Eduardo (2009): Un análisis de la estructura institucional de protección de datos en España en *Revista para el análisis del derecho*. INDRET 2/2009. Disponible en: http://dialnet.unirioja.es/servlet/articulo?codigo=2965016

Martínez, Martínez, Ricard (2007): "El derecho fundamental a la protección de datos: Perspectivas" en *Revista de internet derecho y política*. Agosto 2007 pp. 1- 15

Millán, Salas, Francisco; Peralta Ortega, Juan Carlos (1995): "El derecho de autodeterminación informativa como derecho de la personalidad o derecho fundamental" en *Cuadernos de Estudios Empresariales*, Nº 5, Madrid, pp 203-222.

Mora Antonio (2003): "El libro del defensor del pueblo" Madrid 2003. Pp 1-61.

Murillo de la Cueva, Lucas, Pablo (1999) "La construcción del derecho a la autodeterminación informativa" en *Revista de Estudios Políticos*. Número 104. Abril – Junio.

Murillo de la Cueva, Lucas. (2004): "Derechos fundamentales y avances tecnológicos. Los riesgos del Progreso" en *Boletín Mexicano de Derecho Comparado nueva serie*, año XXXVII número 109 enero – abril de 2004 pp.71-110.

Najera, Montiel, Javier (2008) "El thelos de la protección de los datos personales ante el derecho al acceso a la información". En *Ius Humani. Revista de Derecho*, Volumen 1 (2208/2009) Enero 2008 pp. 177-199.

Nieves Saldaña, María (2011): "El derecho a la privacidad en los estados unidos: Aproximación Diacrónica a los intereses constitucionales en juego" en *UNED Teoría y Realidad Constitucional*. Número 28, 2011, pp. 279-312.

Nogueira, Alcalá Humberto (1998): "El derecho a la privacidad y a la intimidad en el ordenamiento jurídico chileno" en *Ius et Praxis*. Universidad de Talca, Chile, Volumen 4 número 2, 1998

Lucas Murillo de la Cueva, Pablo (1990): *El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática.* Madrid, Tecnos.

ONG Meta (12 de Septiembre de 2013), Observatorio Iberoamericano de Protección de Datos*:* Declaración de Santiago, hacia una unificación de criterios sobre seguridad y protección de datos en Internet. http://oiprodat.com/declaracion-de-santiago/ Fecha de última consulta: 24/Noviembre/2013

Palacios, González, María Dolores (2012). "El poder de autodeterminación de los datos personales en Internet" en *Revista de Internet derecho y política.* Número 14, Mayo 2012. Pp. 61 – 74. Disponible en: http://www.uoc.edu/ojs/index.php/idp/article/viewFile/n14-palacios/n14-palacios-es Fecha de última consulta. 24/Noviembre/2013.

Paladella Salord, Carlos (1999): "Datos personales contenidos en Bases de Datos y Registros Electrónicos" en *REDI Revista Electrónica de Derecho Informático.* Editorial vLex, Número 7, Febrero 1999.

Peña, Antonio (1999): "Hacia la universalidad del derecho informático. Sueño o Realidad" en *REDI Revista Electrónica de Derecho informático*, editorial vLex, número 16 Noviembre 1999. Pp.4

Pérez, Lillo, Claudio. (2013): "Modificaciones para una efectiva regulación de datos personales en Chile" en *Centro de Estudios del Desarrollo,* Informe 1041. Disponible en: http://www.asuntospublicos.cl/2013/04/modificaciones-para-una-efectiva-regulacion-de-datos-personales-en-chile/ Fecha última consulta: 25 de Noviembre de 2013.

Peyrano, Guillermo, "Banco de Datos y tratamiento de datos personales. Analisis de algunas problemáticas fundamentales". en *REDI Revista electrónica de Derecho Informático.* Editorial vLex, Número 34, Mayo 2001.

Peyrano, Guillermo. (2003): Nuevas problemáticas del tratamiento de datos personales. El tratamiento de informaciones que proporcionan datos persona en: REDI Revista Electrónica de Derecho Informático, Editorial vLex, número 58. Julio 2003. Pp.20

Quezada, Rodríguez, Flavio. (2012): "La protección de datos personales en la jurisprudencia del Tribunal Constitucional de Chile." en *Revista Chilena de Derecho y Tecnología* Centro de Estudios en Derecho Informático – Universidad de Chile. Volumen 1 N 1 (2012) pp. 125-147

Rajevic Mosier, Enrique. (2010) "Protección de datos y transparencia en la administración pública chilena: inevitable y deseable ponderación". En *En foco,* ponencia presentada en el taller "Chile y la protección de datos personales" organizado por expansiva. Disponible en http://www.consejotransparencia.cl/consejo/site/artic/20121213/asocfile/20121213161557/

pdp_transparencia_rajevic_expansiva2011.pdf Fecha de última consulta: 24/Noviembre/2013.

Reusser, Monsalvez, Carlos (2007) "Chile y el Derecho de Acceso a la Información. Notas sobre problemas prácticos y gestión del conocimiento" en *Centro de Estudios en Derecho Informático*, Ponencia presentada en el Seminario Internacional "El derecho de Acceso a la Información Pública" realizado en la Facultad de Ciencias de la Información de la Universidad Complutense de Madrid 27 y 28 de Junio 2007. Disponible en: http://www.cedi.uchile.cl

Ruiz Martínez Esteban. (2002) "España: El derecho a controlar la información personal." REDI Revista de derecho informático, Editorial vLex, número 49. Agosto 2002. Pp. 1-15.

Silvina, Dorrego, Claudia. "La desaparición forzada de datos personales: Su venta ilegal y la prevención en el derecho internacional". *REDI Revista Electrónica de Derecho informático,* editorial vLex, Número 28; Noviembre 2000.

Slavin, Diana de. (1999): *Mercosur: la protección de los datos personales: privacidad versus derecho a la información: Régimen legal en el Mercosur y en la Unión Europea: Habeas data.* Buenos Aires, Editorial Depalma.

Suarez Crothers, Christian (2000): "El concepto de derecho a la vida privada en el derecho anglosajón y europeo." en Revista de Derecho (Valdivia) Volumen XI 2000, pp. 103-120.

Urioste, Mercedes (2003) "Argentina: Protección de datos personales" en *REDI Revista Electrónica de Derecho Informático.* Editorial vLex, Número 53, Julio 2003.

BIBLIOGRAFIA CITADA.

Aced, F. E., 2004. La situación en España.. En: *¿Seguridad, privacidad, confidencialidad? El desafio de la protección de datos personales.*. Montevideo: Trilce, p. 222.

AGPD, 2013. *AGPD.es*. [En línea] Available at: http://www.agpd.es/portalwebAGPD/index-ides-idphp.php [Último acceso: 03 Noviembre 2013].

Arenas, R. M., 2005. Integración Europea y protección de datos personales. Las garantías especificas del Derecho a la Protección de datos personales.. *Afdua 2005*, p. 35.

Arrieta, R., 2009. Chile y la protección de datos personales: Compromisos internacionales. En: *Chile y la protección de datos personales ¿Están en crisis nuestros derechos fundamentales?* . Santiago - Chile: Ediciones Universidad Diego Portales. , p. 102.

Bahamonde Guasch, C., 2008. Los datos personales en Chile: Concepto, Clasificación y Naturaleza Juridica.. *Ius Novum,* Issue I, p. 45.

Banda Vergara, A., 2000. Manejo de datos personales. Un límite al derecho a la vida privada.. *Revista de Derecho,* Volumen XI, pp. 55 - 70.

Biblioteca del Congreso Nacional, C., 2013. *BCN*. [En línea] Available at: http://www.leychile.cl/Navegar/scripts/obtienearchivo?id=recursoslegales/10221.3/2468/7/HL19628.pdf [Último acceso: 29 Octubre 2013].

Bru, C. e., 2007. La protección de datos en España y en la Union Europea. Especial referencia a los mecanismos juridicos de reacción frente a la vulneración del derecho a la intimidad.. *Revista D´Internet, Dret I Politica (Revista de Internat, derecho y politica).* , Issue 5, pp. 78 - 92.

Castillo Jimenez, C., s.f. Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información.. *Derecho y conocimiento,* Volumen 1, pp. 35 - 48.

Castro Martines, Karla. Moreno Carrasco, Diego, 2012. *Desafios de la legislación chilena frente a la protección de datos personales.*. s.l.:s.n.

Cea Egaña, J. L., 1996. El derecho constitucional a la intimidad. *Revista Gaceta Juridica* , Issue 198, p. 27 y siguientes. .

Cerda Silva, A., 2003. La autoridad de Control en la legislación sobre protección frente al tratamiento de datos personales. En: L. D. Abarca, ed. *Tesis para optar al grado de Magister en Derecho.* Santiago: s.n., pp. 1 - 245.

Cerda, A., 2013. *Digital Rights Lac.* [En línea]
Available at: http://www.digitalrightslac.net/es/chile-proyecto-de-ley-de-proteccion-de-vida-privada-es-un-retroceso-para-ciudadanos-e-industria/
[Último acceso: 15 Agosto 2013].

Cerda, S. A., 2006. Mecanismos de Control en la Protección de datos en Europa.. *Ius et Praxis,* Issue 12, pp. 221 - 251.

Cerda, S. A., 2011. El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la unión europea.. *Revista de Derecho de la Pontificia Universidad Catolica de Valparaiso,* Issue XXXVI, pp. 327 - 356.

Cerda, S. A., s.f. Autodeterminación Informativa y Leyes sobre protección de Datos.

Chen Mok, S., 2010. Privacidad y Protección de Datos: Un analisis de legislación comparada. *Dialogos. Revista Electronica de Historia.* , 11(1), pp. 111 - 152.

DataOmbudsmannensByra, 2013. *Tietosuojavaltuutetun toimisto.* [En línea]
Available at: http://www.tietosuoja.fi/27307.htm
[Último acceso: 03 Noviembre 2013].

Datatilsynet, 2013. *Datatilsynet.dk.* [En línea] Available at: http://www.datatilsynet.dk/english/ [Último acceso: 03 Noviembre 2013].

Desantes, J. M., 1992. El derecho fundamental a la intimidad. *El derecho a la intimidad y a la vida privada y los medios de comunicación social.,* Revista Estudios Publicos, del centro de estudios públicos.(46).

Donoso, A. L., 2013. Derechos Humanos y Derechos fundamentales en la sociedad en Red. . En: P. R. Olmedo, ed. *Ciudadanas 2020 II* . Santiago: s.n., p. 262.

Ekmekdjlan, Miguel Angel y Pizzolo, Calogero., 1995. *Habeas Data. El derecho a la intimidad frente a la revolución informatica.*. Buenos Aires: Ediciones de Palma.

Fernández, H. V., 2006. Protección de Datos personales en Chile.. *Memoria para optar al grado academico de licenciado en ciencias juridicas y sociales.* .

Ferreiro Yazigi, A., 2013. *Consejo Transparencia.* [En línea] Available at: http://www.consejotransparencia.cl/proteccion-de-datos-personales-los-desafios-de-una-nueva-legislacion/consejo/2009-12-14/114907.html [Último acceso: 14 Agosto 2013].

Ferreiro, A., 2013. *Consejo para la Transparencia.* [En línea] Available at: http://www.cplt.cl/cplt-expuso-sobre-proyecto-de-ley-de-proteccion-de-datos-personales/consejo/2012-11-14/152357.html [Último acceso: 13 Agosto 2013].

Francisco., C. C., 1997. Analisis del Anteproyecto de Ley sobre protección de datos personales elaborado por el Ministerio de Justicia (1990 - 1994). *Ius et Praxis Universidad de Talca, Facultad de Ciencias Juridicas y Sociales.* , Issue Año 3 número 1, pp. 201 - 207.

Garcia Gonzalez, A., 2007. "La protección de datos personales: Derecho fundamental del siglo XXI un estudio comparado". *Boletin Mexicano de Derecho Comparado.*, Año XI(120), pp. 743 - 778.

Gregorio, C., s.f. Protección de datos personales: Europa VS. Estados Unidos. Todo un dilema para América Latina.. p. 27.

Hernandez, V. R., 1990. *La tutela de los derechos fundamenales.* San Jose de Costa Rica. : Juricentro.

Herrera Bravo, R., 2001. La protección de datos personales como garantía básica de los derechos fundamentales.. pp. 1 - 12.

Herrera Bravo, R., Septiembre 2001. Chile: ¿Por qué la protección de datos personales es una garantía básica de los Derechos Fundamentales?. *REDI Revista Electronica de Derecho Informatico,* Issue 38, pp. 1 - 15.

ICO, 2013. *Information Commissioner´s Office.* [En línea] Available at: http://www.ico.org.uk/ [Último acceso: 02 Noviembre 2013].

IFAI, 2013. *IFAI.* [En línea] Available at: http://inicio.ifai.org.mx/_catalogs/masterpage/ifai.aspx [Último acceso: 03 Noviembre 2013].

Jaña Tapia, W. A., 2003. Análisis legal comparativo de la protección de datos personales a nivel latinoamericano.. En: *Memoria de prueba para optar al grado de licenciado en ciencias juridicas y sociales..* Santiago.: http://www.tesis.uchile.cl/tesis/uchile/2003/jana_w/html/index-frames.html.

Jervis Ortiz, P., 2002. *Ponencia pronunciada en Seminario Datos personales en Chile. El nuevo regimen normativo..* Santiago : s.n.

Jijena Leiva, R., 2001. La ley chilena de protección de datos personales. Una visión crítica desde el punto de vista de los intereses protegidos.. En: J. W. Silva, ed. *Tratamiento de datos personales y protección de la vida privada. Estudios sobre la Ley N°19.628 sobre protección de datos de caracter personal..* Santiago de Chile: Ediciones Universidad de los Andes, pp. 85 - 111.

Jijena, R. J., 2001. Sobre la no protección de la Intimidad en Chile.. *REDI REvista Electronica de Derecho informatico.*, Issue 39, Octubre 2001. , p. 12.

Jurisprudencia, 1993. *Revista de Derecho y Jurisprudencia,* XC(2), pp. 164 - 174.

Lara, Juan Carlos; Vera, Francisco; Soto, Barbara, 2011. *Privacidad y nuevas tecnologías, regulación chilena y propuestas de politica pública. ,* Santiago: ONG Derechos Digitales. .

Lucas Murillo, P., 1990. *El derecho a la autodeterminación informativa.* Madrid España: Tecnos.

Martorelli - Editorial Planeta. (1993).

Matus, A. J., 2010. *La relación entre el derecho al acceso a la información pública y la protecciónd e los datos personales. ,* Santiago, Chile: Fundación Pro Acceso.

Ministerio de Justicia y Derechos Humanos; Presidencia de la nación, 2013. *Ministerio de Justicia y Derechos Humanos. Presidencia de la Nación..* [En línea] Available at: http://www.jus.gob.ar/el-ministerio/mision.aspx [Último acceso: 02 Noviembre 2013].

Muñoz, A. J., 1998. *Los limites de los Derechos fundamentales en el Derecho Constitucional Español.* Pamplona - España: Aranzadi .

Murillo, D. l. C. L., 1990. *El derecho a la autodeterminación informativa.* Madrir: Tecnos.

Nacional, C., 1996. *Informe Comisión de Constitución, Legislación y Justicia de la Cámara de Diputados. Sesión tercera, 04.06.1996.* Valparaiso. : s.n.

Nacional, C., Tercer tramite, sesión 18, anexo de documentos. Informe de la Comision de Constitución, Legislación, Justicia y Reglamento del Senado. . En: s.l.:s.n., p. 2111.

Nogueira Alcalá, H., 1997. Reflexiones sobre el establecimiento constitucional del Habeas Data y del Proyecto en tramitación parlamentaria sobre la materia.. *Ius et Praxis,* 3(1), pp. 265 - 284.

Nogueira Alcala, H., 1998. El derecho a la privacidad y a la intimidad en el ordenamiento juridico chileno.. *Ius et Praxis Universidad de Talca,* 4(2), pp. 65 - 106.

Nogueira Alcala, H., 2004. Pautas para superar las tensiones entre los Derechos a la Libertad de Opinión e Información y los Derechos a la Honra y la Vida Privada. *Rev. derecho (Valdivia)* - *Scielo,* pp. 139-160.

Nogueira, A. H., 2003. *Teoria y dogmatica de los derechos fundamentales.* Mexico: Universidad Nacional Autonoma de Mexico.

ONG Derechos Digitales; Vera, Francisco; Cerda, Alberto. , 2011. *Minuto de Discusión: Proyecto de Ley que introduce modificaciones a la Ley N° 19.628, sobre protección de la vida privada y protección de datos de caracter personal.* , Santiago.: s.n.

Perez Luño, A., 1989 . Nuevos derechos fundamentales de la era tecnologica: La libertad informatica.. *Anuario de Derecho Publico y Estudios Politicos,* Issue 2.

Pérez Pérez, A., 2004. La situación en Uruguay. En: *¿Seguridad, privacidad, confidencialidad? El desafio de la protección de datos personales.* . Montevideo: Trilce, p. 222.

Perez, Antonio; Losano, Mario; Guerrero, Maria Fernanda, 1989. *Libertad informativa y leyes de protección de datos personales.*. Madrid - España: Centro de estudios Constitucionales. .

Perez, L. A., 1995. *Los derechos fundamentales.*. Madrid - España: Tecnos S.A.

Puccinelli, O., 1999. *El habeas data en Indoiberoamérica.* Bogota: Temis.

Pucinelli, O., 1992. Tipos y Subtipos de Habeas Data en el Derecho Constitucional Latinoamericano. . En: *Suplemento de Derecho Constitucional, ley numerp 135.* . Argentina: s.n.

Rajevic Mosler, E., 2011. *Recomendaciones del consejo para la transparencia sobre protección de datos personales por parte de los organos de la administración del Estado.* , Santiago: s.n.

Rajevic, E. M., 2011. Protección de datos y transparencia en la administración pública chilena: Inevistable y deseable ponderación. . En: *Reflexiones sobre el Uso y Abuso de los datos personales en Chile.* . Santiago : Expansiva, p. 184.

Real Academia, E., 2009 - 2010. *http://www.rae.es/rae.html.* [En línea] Available at: http://lema.rae.es/drae/?val=dato [Último acceso: 27 Julio 2012].

Reusser, M. C., s.f. Privacy, Riservatezza, Intimidad y Autodeterminación Informativa: El camino hacia el derecho fundamental a la protección de datos. . En: *II diploma de Postitulo en Derecho Informatico.*. Santiago : Universidad de Chile, p. 12.

Reusseur Monsálvez, C., s.f. Privacy, Riservatezza, Intimidad y Autodeterminación Informativa: El camino hacia el derecho fundamental a la protección de datos.. Volumen II Diploma de Postitulo en Derecho Informatico..

Reyes Olmedo, Patricia. , 2011. La Sociedad Red y el Gobierno de la Información. . En: *Ciudadanas 2020.* I ed. Santiago: LOM, pp. 193 - 25.

Sanchez Bravo, a., 1998. *La protección del derecho a la libertad informatica en la Union Europea.* Secretariado de publicaciones ed. Sevilla - España : Universidad de Sevilla .

Sanchez Bravo, Á., 1998. *La protección del derecho a la libertad informatica en la Unión Europea.* Sevilla - España: Secretariado de publicaciones. .

Sarra, V. A., 2000. *Comercio electronico y derecho: Aspectos juridicos de los negocios en internet.*. I edición. ed. Buenos Aires, Argentina: Astrea.

Silva Cimma, E., 1994. *Derecho Administrativo y Chileno Comparado. El control Publico.* Santiago: Editorial Juridica.

Suarez Crothers, C., 2000. El concepto de derecho a la vida privada en el derecho anglosajon y europeo. *Revista de Derecho ,* Volumen XI, pp. 103 - 120.

Tellez, J., 2004. *Derecho Informatico.* Tercera Edición ed. Mexico: McGraw Hill / Interamericana Editores S.A.

Uicich, R., 2004. La situación en Argentina. En: *¿Seguridad, privacidad, confidencialidad? El desafio de la protección de datos personales.* . Montevideo : Trilce, p. 222.

URCDP, 2013. *Unidad reguladora y de control de datos personales.*. [En línea] Available at: http://www.datospersonales.gub.uy/inicio/institucional/que-es-la-urcdp/ [Último acceso: 2 Noviembre 2013].