Universidad de Chile
Facultad de Derecho
Departamento Derecho Comercial

DERECHO AL OLVIDO: UNA APROXIMACIÓN DESDE EL ANÁLISIS DEL CASO COSTEJA AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN EUROPA. IMPORTACIÓN, APLICACIÓN Y PROBLEMÁTICAS EN LA LEGISLACIÓN NACIONAL.

Memoria para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales.

PAMELA FUENTEALBA PALOMERA

PROFESOR GUÍA: SR. CLAUDIO MAGLIONA

Santiago, Chile.

2020

A mi familia y Carmina, por su cariño.

Agradecimientos

Mis más sinceros agradecimientos a mis padres, Jessica y Antonio, por su amor y apoyo incondicional, ya que siempre estuvieron para mí, educándome, conteniéndome y potenciando mis capacidades.

A Carmina, quien fue fundamental en la culminación de este trabajo, por su paciencia y dedicación, porque sin sus consejos y ayuda esto no hubiese sido posible.

A mi familia por sus palabras de apoyo y aliento, por creer siempre en mí sin importar lo que sucediera.

A María Gracia, por su ayuda y colaboración en la etapa final de este largo camino.

Finalmente no puedo más que agradecer a la gran institución que me acogió todos estos años, Universidad de Chile, por todo lo que me enseñó que fue más allá de lo que aprendí en sus aulas y a cada persona que crea esta Universidad: mis profesores, compañeros y funcionarios y, especialmente, al profesor Daniel Valenzuela por su guía y dedicación durante el taller de memoria, y al profesor Claudio Magliona por su buena disposición y apoyo académico otorgado en el desarrollo del presente trabajo.

TABLA DE CONTENIDO

INTRODUCCIÓN

El derecho como ciencia social se basa principalmente en el estudio del comportamiento del hombre en particular y de su relación con sus pares. El entorno dentro del cual se desenvuelve el hombre se encuentra constantemente en variación, la cual puede derivar de su voluntad o bien provenir de elementos externos a ella. Un ejemplo de lo anterior es el avance tecnológico que hemos experimentado en las últimas décadas, el cual ha traído consigo una masificación de las comunicaciones y ha permitido el acceso a una cantidad variada de información, la principal incidencia en ello fue la llegada de internet y la propagación en su acceso. Hoy en día es considerado como un bien de consumo necesario para la mayoría de la sociedad ya que cumple diversas funciones, dentro de las cuales encontramos el hecho de ser un medio de comunicación masivo, a gran escala e inmediato, además de ser vital en las relaciones sociales. Esta última es la característica que nos interesa.

Se hace necesario por tanto un cuerpo normativo que controle de alguna forma el uso de internet, para que no se transforme en abuso indiscriminado en el tráfico de información, tema que compete al presente trabajo. No obstante, una de las problemáticas que se nos hace necesario patentar es la extraterritorialidad de la hipotética normativa, ya que la información en internet recorre todo el mundo y existen distintos servidores dentro de él, problema que ahondaremos en su oportunidad.

No existe una forma eficaz de controlar el tráfico de datos, debido a lo masivo que se ha vuelto su uso. Y al no existir una normativa respecto al manejo de la información en las plataformas virtuales, se deja al usuario que accede a ella desprovisto de cualquier protección, pudiendo prestarse este uso para cualquier cosa.

Se ha dicho que internet no olvida, que la información que se sube a ella es incontrolable en su tráfico y que nunca puede ser totalmente eliminada debido a la masividad de usuarios con los que cuenta.

Si bien internet ofrece beneficios como medio de comunicación, a su vez genera riesgos, los cuales surgen principalmente por el mal manejo, control y utilización de información, ya sea porque esta es tergiversada, sacada de contexto, distorsionada, errónea, imprecisa, ofensiva o bien desactualizada, lo cual puede ocurrir tanto de forma negligente como maliciosa, siendo dañina para alguna persona o grupos de ellas.

En lo que hoy en día se conoce como redes sociales, no es posible controlar el intercambio, destinación o el trayecto de la información que subimos en la web de forma voluntaria. Entonces, desde esa mirada

podemos concluir que en menor medida somos capaces de controlar si un tercero sube información sobre nosotros, sin embargo, ambos factores conforman nuestra huella digital.

En ocasiones, no es posible revisar el contenido personal de algún elemento subido a internet por parte de terceros, por lo que se está expuesto a ser víctimas de la expansión de la información y mal uso de esta, sin haberlo autorizado.

El derecho al olvido nace como una alternativa posible para poder solucionar estos problemas y de alguna forma controlar esta situación, sacando de internet el estado de naturaleza que existe en él, mediante normativas con carácter ex post sobre el manejo de información.

Luego de enseñarle al lector sobre el panorama general del derecho al olvido, su extensión y alcances, será necesario traerlo a la realidad nacional y examinar cómo se recoge este derecho en nuestro país. Principalmente abordaremos el punto de vista legislativo y como la doctrina intenta llenar los vacíos y problemas que la ley presenta, se criticará las falencias que presenta la ley para luego referirse a los proyectos de ley que se encuentran en trámite en el parlamento, así como también veremos casos suscitados en nuestros tribunales relativos al derecho al olvido.

El presente trabajo tiene como principales objetivos:

✓ Acercar al lector común el conocimiento de tecnicismos del mundo virtual, para que se familiarice con el vocabulario y pueda comprender de mejor forma el presente tema.

✓ Informar al lector sobre el Derecho al Olvido, el cual se encuentra desplazado de nuestra realidad como país, sin embargo, existe una luz de esperanza para que en algún momento se recoja y aplique, debido a su urgencia y relevancia considerando el mundo en el que hoy vivimos.

✓ Informar al lector de cómo se recoge esta institución en el viejo continente, como se ha desarrollado en él, y la visión actual que se tiene al respecto, tomándolo así, como un posible modelo a seguir.

✓ Informar al lector sobre el escenario político y legal en el que se instala el derecho al olvido en nuestro país.

✓ Criticar las carencias de la legislación nacional y explicar la repercusión de aquellos errores, y tras esto, proponer soluciones de carácter personal como las que presentan los parlamentarios en las distintas mociones que se han efectuado frente al tema y analizar jurisprudencia relativa al tema.

Capítulo 1: Panorama General del Derecho al Olvido

1.1 Conceptos Claves

Con la finalidad de comprender mejor el presente trabajo, creemos que, en primer lugar, es necesario explicar y precisar algunos conceptos respecto al mundo del internet y la privacidad, ya que muchos de ellos pueden ser desconocidos.

Para comenzar, empezaremos por lo más básico, según González, el **internet**, *es la red mundial de redes de computadores que permite comunicarse entre sí compartiendo información y datos. Es una gran red de ordenadores, cada uno de ellos independiente y autónomo.* Básicamente, estos ordenadores se encuentran conectados entre sí a través de proveedores de servicios. Como lo señala Rodríguez (2014), Internet ha evolucionado de manera muy rápidamente y hoy integra múltiples servicios, permitiendo el acceso a la Word Wide Web, una red informática mundial comparable a una biblioteca llena de páginas de información.

Dentro de los actores que participan en esta red de internet encontramos a los **proveedores de servicios**, estos corresponden a las empresas que brindan conexión a internet a sus clientes. Se pueden clasificar en **proveedores de acceso**, que permiten la conexión a la red; **proveedores de enlace**, que proporcionan los mecanismos de transmisión y **proveedores de Hosting**, que proporcionan un espacio en el disco duro para almacenar información. Otro de los actores de internet son los **titulares de registro de dominio**. Se entiende por registro de dominio a los signos representativos de los distintos sitios de internet. Por otro lado, nos encontramos con los **proveedores de contenidos**, que son personas naturales o jurídicas que ponen a disposición de los usuarios contenidos y/o aplicaciones en internet a través de medios propios o de terceros. (Moya, 1993)

Por último, uno de los actores más importantes en la red son los **usuarios**, siendo estos emisores y receptores de información que se encuentra en la web, y quienes controlan de cierta forma internet, al poder ellos escoger los contenidos a los que desean tener acceso y aquellos que quieren incorporar a la red.

Continuando en el mundo del internet, una de las herramientas técnicas más importantes utilizadas en él son los **motores de búsqueda**, según lo indica Torres (2003), estos corresponden a un sistema que facilita el hallazgo de archivos en servidores web, además de ayudar en la navegación gracias a su "araña web", mediante la introducción de palabras claves. Estos buscadores muestran como resultados una lista de direcciones o páginas web que contienen las palabras claves que fueron buscadas por los usuarios.

Otro concepto relevante es la **indexación**, este consiste en agregar una o más páginas web a las bases de datos que poseen los motores de búsqueda, para que estas aparezcan dentro de los resultados que arroja aquel. Sin la indexación la ubicación de estas páginas por parte de los usuarios sería extremadamente compleja, puesto que, para lograr ingresar al contenido deseado tendrían que conocer el enlace exacto de la página web que se quiere visitar para poder acceder a ella (Pérez y Merino, 2018).

Es importante también definir dos herramientas técnicas de gran relevancia para la aplicación del Derecho al Olvido, puesto que estas han sido puestas como parte de las soluciones que se han dado en casos de contingencia mundial. La primera de ellas es **robots.txt.,** según respuesta Google este *proporciona información a los rastreadores de los buscadores sobre las páginas o los archivos que pueden solicitar o no de tu sitio web*.

El segundo concepto corresponde a los **metatags**. Estos son identificadores ocultos o etiquetas HTML que son insertadas en el encabezado de una página web e invisibles para los usuarios. Representan gran utilidad para los buscadores, ya que contienen una referencia de la página, que ayudan a mejorar el listado de los resultados de los mayores buscadores (Senso y De La Rosa 2003).

Otro concepto que nos parece necesario explicar en el contexto de la tecnología son los **datos**, esta palabra proviene del latín *datum* que significa "lo que se da". El sitio de Informática de Google lo define: *Es un valor o referente que recibe el computador por diferentes medios, estos representan la información que el programador manipula en la construcción de una solución o en el desarrollo de un algoritmo*. Al asociarse por determinadas materias se forma un conjunto de datos también conocidos como banco de datos, que puede ser utilizado por varias personas. En ellos la información se encuentra clasificada y ordenada de acuerdo con diferentes parámetros, con la finalidad de que al momento de ser solicitada con diversos fines sea más fácil encontrar y otorgar dicha información.

Relacionado con lo anterior existen los **datos personales**, la comunidad Europea lo define como *toda aquella información relativa a una persona física, que lo identifica o lo hace identificable*. Son en definitiva, lo que le dan identidad, muestran sus características, señalan su origen, edad, profesión u oficio, entre otros y señalan además aspectos sensibles sobre la persona, como su ideología, credo, orientación sexual y más (Instituto Federal de Acceso a la Información Pública de México, 2014). Hoy en día con la expansión de las redes sociales e internet en general, muchas veces se produce un uso poco responsable de los datos personales. Lo ideal sería que existiera conformidad por parte de la persona a la hora de suministrar los datos personales, es por esto mismo que se han creado legislaciones que se ocupan de la seguridad y regulación respecto de la información personal de los individuos. Dichas legislaciones pueden contener en sus cuerpos legales lo que se conoce como **habeas data**, este es un

derecho constitucional que puede utilizar y hacer valer cualquier individuo que considere que su información personal debe ser eliminada o rectificada si es que esta es falsa, resulta obsoleta por el paso del tiempo o ha perdido totalmente su utilidad (Quiroz, 2016).

Así entonces, el habeas data funciona en la sociedad como una garantía acerca de la correcta manipulación e intercambio de los datos personales que se hallan en manos de terceros. Gracias a él se pueden impedir abusos a los derechos de honra, de intimidad de la vida privada y familiar, entre otros, o corregir datos que no sean verdaderos y que como tales le ocasionen al individuo algún perjuicio.

Relativo de igual forma al tema de los datos, cabe precisar lo que se entiende por **banco de datos**, concepto de relevancia en el desarrollo del presente trabajo, y que podemos definir como un conjunto de datos, de informaciones que son agrupadas y mantenidas en un mismo soporte a modo de facilitar su acceso, sin embargo, en términos más específicos y en relación con la importancia que la tecnología tiene hoy en día, la idea de banco de datos suele aplicarse a sistemas informáticos que guardan información y que permiten a los usuarios acceder a esos datos fácilmente. (Bembibre, 2012)

1.2 Definición y características del Derecho al Olvido

El derecho al olvido fue definido por el Tribunal de Justicia Europeo como *el derecho de los titulares de datos personales a exigir la cancelación u oposición al tratamiento de dichos datos realizado por los servicios de búsqueda de internet, cuando el tratamiento sea inadecuado, no pertinente o excesivo en relación con los fines del tratamiento y cuando los datos tratados no estén actualizados o se conserven durante un período superior al necesario; incluso cuando dicho tratamiento pudo ser licito en su origen.*

De la definición anterior se desprende entonces que la información de carácter personal que se pretende proteger, en principio, debe generar un daño, ya sea porque se encuentra tergiversada, sacada de contexto, distorsionada, errónea, imprecisa, ofensiva o bien desactualizada, y que su correspondiente eliminación debe obedecer a diversos criterios legales que expondremos más adelante.

Dentro de las características que podemos encontrar en este derecho destacan principalmente las siguientes:

a. **No es absoluto**: Es un derecho que no se concede en su totalidad plena debido a que por lo general, entra en conflicto con otros derechos constitucionales, principalmente con la libertad de expresión y libre circulación de la información. De todas formas, la acogida en mayor o menor

medida de dicho derecho dependerá del enfoque que posea un determinado país, el nivel de importancia que se le otorguen a ciertos derechos y como se encuentren consagrados en su carta fundamental.

b. **No es renunciable**: La facultad de ejercer este derecho, desde el punto de vista procesal, no debiera ser sometida a la renuncia anticipada y voluntaria del afectado, ya que los derechos que se buscan proteger son de alta importancia y por tanto son de orden público.

c. **Es inalienable**: La facultad de hacer valer este derecho, desde un punto de vista netamente procesal, solo puede ser ejercida por la persona afectada por la publicación de sus datos personales en internet, sin que de alguna forma se pueda enajenar o transmitir la legitimación activa.

d. **Incipiente**: En diversas situaciones se ha cuestionado la existencia misma del derecho al olvido. Ha sido más bien un derecho que se ha ido consagrando y construyendo con el transcurso del tiempo, en virtud de la masificación del acceso y permanencia de usuarios en internet, así como el aumento exponencial en el intercambio de información entre actores de diversas partes del mundo.

e. **Es un derecho protector de garantías constitucionales**: El derecho al olvido busca proteger ciertas áreas de la libertad individual como lo son básicamente la dignidad, la honra, privacidad e incluso algunas veces la intimidad de la persona, derechos de suma importancia en cualquier sociedad democrática. Hoy en día no se concibe sociedad que no proteja a los ciudadanos de las amenazas que vulneren o pongan en peligro sus derechos.

f. **Independiente**: Es una característica que aún no se desarrolla plenamente, siendo más bien un ideal el hecho de ser considerado como un derecho autónomo. El derecho al olvido al ser un derecho insipiente que no se ha desarrollado de forma plena, sino que, al contrario, se encuentra relacionado directamente con el derecho de cancelación. En efecto, en la sentencia del TJUE respecto de Google vs AEPD y Costeja, en ningún momento se limita a señalarnos que evidentemente existe un derecho propiamente tal con el nombre de ‘’Derecho al Olvido’’, sino más bien hace hincapié en el derecho de cancelación.

g. **Es un derecho que depende de la situación sociocultural de la sociedad que lo recoge**: Los países tienen distintas legislaciones y recogen de distinta forma los derechos constitucionales, en virtud de esta diferencia, se inclinan algunas veces por la protección de ciertos bienes jurídicos que por otros. Notable es el caso de Estados Unidos en que en la primera enmienda de la Carta

Fundamental de Derechos se encuentra consagrado el derecho a la libertad de expresión, por lo mismo a la hora de comparar dicho derecho con la privacidad, el cual se encuentra en la cuarta enmienda, se va a preferir el primero por una cuestión de primacía existente entre estas. Estados Unidos le entrega a cada ciudadano la libertad de controlar su propia privacidad, por lo tanto, es evidente que el derecho al olvido no tendrá cabida en una legislación de ese tipo o si llegase a implementarse su aplicación será limitada. (Sandoval, 2016).

1.3 Panorama general de la Visión Europea versus la Visión Americana del Derecho al Olvido.

Durante el desarrollo del derecho al olvido como tal han surgido principalmente dos enfoques respecto a su regulación y aplicación.

Por un lado, existe una visión más liberal, como es el caso de Estados Unidos en cuya Carta Fundamental de Derechos (1787), existe una ponderación de estos que, como mencionábamos anteriormente, prefiere el derecho a la libertad de expresión consagrado en la primera enmienda por sobre el derecho a la privacidad de las personas establecido en la cuarta enmienda, pasando a ocupar este último un segundo lugar en la mayoría de los casos en que ambos derechos entran en pugna.

La visión norteamericana brinda libertad absoluta a las personas para poder controlar su privacidad y a su vez de como resguardarla frente a invasiones de terceros. De alguna forma podemos notar como el Estado Americano evita inmiscuirse en situaciones relacionadas con estos temas, salvo en casos muy excepcionales.

En contraposición a lo anterior nos encontramos con el enfoque europeo, en el cual, el derecho a la privacidad es un aspecto de la libertad personal y un componente de la dignidad humana.

Este espíritu es el que se refleja en el artículo 8 de la Convención Europea de Derechos Humanos, el cual señala que "*toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*" señalando en su segundo numeral que "*No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las*

libertades de los demás", reflejo automático de la tradición francesa caracterizada siempre como protectora de sus ciudadanos.

El Derecho al Olvido europeo se gesta en Francia (le droit a l' oubli) y surge principalmente por el registro que se llevaba de los expedientes de aquellas personas que cometían crímenes y eran condenados, el cual se mantenía publicado, incluso tras haberse cumplido con la pena, situación que les ocasionaba un perjuicio innecesario al momento de querer reinsertarse en la sociedad (Rosen, 2012).

Con el tiempo se extendió esta conclusión y comenzó a aplicarse respecto a la divulgación relativa a otros tipos de información de los individuos. Considerando así que la información referente a una persona debiera ser borrada una vez que ha concluido su propósito o finalidad en virtud del cual existía o, dicho de otra forma, cuando no exista argumento racional alguno para seguir publicada y solo afecta a la reputación de la persona. Esa es la idea que se extrae del artículo 6 de la directiva 95/46 de la Unión Europea relativa a la protección de datos personales, el cual dispone que "los Estados miembros dispondrán que los datos personales sean: a) tratados de manera leal y lícita; b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas; c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente; d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados; e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos". Lo señalado anteriormente se reafirma y consolida con lo estipulado en el artículo 12 del mencionado cuerpo legal, ya que en caso de que el tratamiento de los datos relativos a una persona no se realicen en conformidad al artículo 6, se le otorga al sujeto el derecho de exigir a quien controla la información "la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos".

Sin embargo, no es hasta el año 2010 cuando comienza a tomar mayor relevancia e importancia el derecho al olvido como tal, esto a raíz del caso Google vs AEPD y Costeja, el que debido a su alcance, masificación y popularización pone en boga dicho derecho.

En el siguiente apartado se procede a comentar este caso en particular.

1.4 Google vs AEPD

- Los hechos: El ciudadano español Mario Costeja realiza un reclamo frente a la Agencia Española de Protección de Datos Personales (AEPD) en marzo de 2010, la razón de dicho reclamo frente a este organismo español se debe a que cada vez que se ingresaba en los motores de búsqueda Google Spain y Google Inc su nombre, estos inmediatamente arrojaban entre sus principales resultados dos enlaces, donde lo individualizaban con su nombre completo, que dirigían hacia la página web del diario La Vanguardia Ediciones, S.L., se trataba de dos noticias del año 1998 referentes al hecho de que le habían sido embargados sus bienes por deudas que mantenía en materia de seguridad social. Cabe mencionar que esta publicación fue realizada con la finalidad de publicitar dicho remate y así concurrieran muchos postores. (Tribunal de Justicia de la Unión Europea, 2013)

- La pretensión: El señor Costeja en su reclamo solicitó que el medio de comunicación La Vanguardia Ediciones, S.L. modificara o eliminara dicha información relativa a su persona, fundando esto en la obsolescencia de esta, debido a que la deuda ya se encontraba saldada y, a la vez, por el perjuicio que le ocasionaba a su honra y su vida privada. Sin embargo, su reclamo no solo fue dirigido al diario que publicó las noticias, sino que también hacia los motores de búsqueda Google Spain y Google Inc, solicitando que estos realizaran la desindexación de dichas páginas web al momento de ingresar su nombre en dichos buscadores.

- Respuesta de la Agencia Española de Protección de Datos: Frente al reclamo interpuesto por el ciudadano Costeja, en junio de 2010, la AEPD desestimó la pretensión respecto al medio de comunicación La Vanguardia, señalando que "la publicación que esta había llevado a cabo estaba legalmente justificada, dado que había tenido lugar por orden del Ministerio de Trabajo y Asuntos Sociales y tenía por objeto dar la máxima publicidad a la subasta para conseguir la mayor concurrencia de licitadores". Mientras que respecto a la pretensión hecha valer en contra de los motores de búsqueda de Google España y Google Inc la respuesta fue positiva, ya que fue acogida por la AEPD, quien obligó a restringir el acceso a la información relativa al señor Costeja, pues "consideró que quienes gestionan motores de búsqueda están sometidos a la normativa en materia de protección de datos, dado que llevan a cabo un tratamiento de datos del que son responsables y actúan como intermediarios de la sociedad de la información" Añadiendo a dicha fundamentación que la misma AEPD "estaba facultada para ordenar la retirada e imposibilitar el acceso a determinados datos por parte de los gestores de motores de búsqueda cuando

considere que su localización y difusión puede lesionar el derecho fundamental a la protección de datos y a la dignidad de la persona entendida en un sentido amplio, lo que incluye la mera voluntad del particular afectado cuando quiere que tales datos no sean conocidos por terceros".

- Interposición de recursos frente al fallo de la AEPD: La actitud adoptada por Google España y Google Inc. fue la de presentar un recurso ante la Audiencia Nacional en contra de la resolución dictaminada por la AEPD, la cual los determinaba como responsables de tratamientos de datos personales, sin embargo, la Audiencia Española no le dio curso a la tramitación debido a que antes de fallar dicho recurso debía resolver ciertas cuestiones de carácter prejudicial, y que su respuesta dependía "del modo en que debe interpretarse la Directiva 95/46 en el marco de estas tecnologías, que han surgido después de su publicación".

  Es por esto que la Audiencia Nacional plantea al Tribunal de Justicia de la Unión Europea las siguientes cuestiones prejudiciales:

  a) Ámbito de aplicación material de la Directiva 95/46, esta cuestión prejudicial apunta a si se debe considerar que los motores de búsqueda realizan o no tratamiento de datos, y de considerarse afirmativo, saber si los gestores de los mismos deben ser considerados responsables de dicho tratamiento.

  b) Ámbito de aplicación territorial de la Directiva 95/46, esta cuestión prejudicial apunta a saber si la directiva puede ser aplicable al motor de búsqueda Google Search, debido a que no es un establecimiento domiciliado en un estado miembro.

  c) Alcance de la responsabilidad del gestor de un motor de búsqueda en virtud de la Directiva 95/46, esta cuestión prejudicial apunta al hecho de saber si los motores de búsqueda están obligados a eliminar de la lista de resultados de búsqueda los enlaces de páginas webs con la finalidad de proteger los derechos garantizados por la directiva, aun cuando el tratamiento de datos que realizan dichas páginas sea considerado lícito y no se exija la eliminación de dicha información.

  d) Alcance de los derechos del interesado garantizados por la Directiva 95/46, esta cuestión prejudicial dice relación respecto de si el interesado, es decir, el señor Costeja, tiene derecho a exigir que el motor de búsqueda elimine los vínculos de las páginas web que contienen información relativa a su persona debido a que esto le ocasiona un perjuicio.

- Consideraciones del fallo del TJUE y su respuesta a las cuestiones prejudiciales presentadas por la Audiencia Nacional: Respecto al ámbito de aplicación material de la Directiva 95/46, la sentencia señaló que "la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en

Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de «tratamiento de datos personales», en el sentido de dicho artículo 2, letra b), cuando esa información contiene datos personales, y, por otro, el gestor de un motor de búsqueda debe considerarse «responsable» de dicho tratamiento, en el sentido del mencionado artículo 2, letra d).”

Respecto al ámbito de aplicación territorial de la Directiva 95/46, el TJUE señaló que si bien el domicilio del servidor de Google Search (que trataba los datos personales del señor Costeja) se encontraba en Estados Unidos, existía una filial de la misma ubicada en España llamada Google Spain, existiendo entre ambas una vinculación relativa al marketing y la publicidad debido a que sirve como un medio en que se incluye publicidad asociada a patrones de búsqueda al servicio de los usuarios además de la indexación de páginas web. Debido a esto el tribunal estima que “la actividad de promoción y venta de espacios publicitarios, de la que Google Spain es responsable para España, constituye la parte esencial de la actividad comercial del grupo Google y puede considerarse que está estrechamente vinculada a Google Search”, y que por lo tanto “se lleva a cabo un tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro”, concluyendo así que la Directiva 95/46 es aplicable al motor de búsqueda Google.

Respecto al alcance de la responsabilidad del gestor de un motor de búsqueda en virtud de la Directiva 95/46, el TJUE señaló en su resolución que “el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita”.

Finalmente respecto al alcance de los derechos del interesado garantizados por la Directiva 95/46, el TJUE reconoce el derecho de las personas a solicitar a los motores de búsqueda que, bajo ciertos requisitos, eliminen los enlaces de las páginas webs que contienen información sobre ellos, señalando que puede “solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no solo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona”, dando así espacio al Derecho al Olvido.

- Críticas al fallo: Como podemos apreciar la sentencia finalmente establece la obligación a los motores de búsqueda de eliminar aquellos enlaces de páginas webs que contienen información relativa a una persona, mas no ordena la eliminación de la página misma del medio de comunicación que publicó la noticia, por lo que dicha información continúa siendo accesible a todo público que conozca la dirección exacta de dicha página, continuando con la vulneración hacia sus derechos de la dignidad y la privacidad. Esto ocurre en virtud de la matización que debe existir entre los derechos que entran en conflicto, pues el derecho al olvido y los demás derechos que este protege deben convivir de forma equilibrada con la libertad de expresión ya que no se trata de un derecho absoluto.

  Junto a la crítica anterior cabe señalar que la eliminación del enlace solo afectó a los motores de búsqueda Google inc. y Google Spain, ya que por conflictos de territorialidad en cuanto a la aplicación de la normativa, no era posible solicitarle a las demás filiales que tiene Google Search en diversas partes del mundo que eliminaran los enlaces anteriormente referidos, por lo que al momento de ingresar en el motor de búsqueda de Google Chile u otro país, o incluso en otro motor de búsqueda como Yahoo!, seguirán apareciendo en los resultados de búsqueda los enlaces de la página web del diario la Vanguardia.

  En consecuencia, se ha sostenido que como el Derecho al Olvido no es absoluto no existe por sí mismo de forma autónoma, sino más bien solo se concibe como un derecho de cancelación, limitando en forma parcial el acceso a la información y no cumpliendo así el ideal que persigue, que es la eliminación total de datos personales cuando no exista finalidad alguna para su mantención.

- Fundamento legal del fallo: Este caso fue resuelto por el TJUE en base a la Carta de los Derechos Fundamentales de la Unión Europea del año 2000, la cual en el preámbulo señala que "es necesario… reforzar la protección de los derechos fundamentales a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos". Fueron fundamentales los artículos 7 y 8 del capítulo 2 de la mencionada carta, los cuales hablan del respeto de la vida privada y familiar, y la protección de datos de carácter personal respectivamente.

  Pero sin duda alguna, el principal fundamento legal utilizado en la resolución del caso fue la Directiva 95/46 del Parlamento Europeo y del Consejo, que entró en vigencia el 13 de diciembre de 1995, relativa a la protección de datos personales. Esta Directiva era una de las normativas más importantes en Europa hasta hace pocos años respecto a este tema, pues creó "un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). Con ese objeto, la Directiva fijaba límites estrictos para la recolección y utilización de los datos personales y solicitaba la creación, en cada Estado miembro,

de un organismo nacional independiente encargado de la supervisión de cualquier actividad relacionada con el tratamiento de los datos personales".

El ámbito de aplicación de la directiva se establecía en su artículo tercero, el cual estipulaba que recae tanto al tratamiento de datos en medios automatizados como no automatizados. El primero consiste en un conjunto ordenado de datos personales, el cual permite encontrar información relativa a una determinada persona física mediante procedimientos de búsqueda automatizados, como por ejemplo las bases de datos que encontramos en internet respecto a algún tema determinado, mientras que los segundos corresponden a los datos que se encuentran en ficheros en papel. A continuación, el mismo artículo señalaba aquellas excepciones en que, a pesar de tratarse de un tratamiento de datos automatizado o no, la directiva no tenía aplicación, esto ocurría cuando el tratamiento de datos era ejercido por una persona en ámbitos particulares o domésticos, o bien, cuando se trataba de actividades de seguridad pública o del Estado, o la defensa de estos.

Uno de los artículos de gran relevancia de esta directiva era el sexto ya que establecía los principios relativos a la calidad de los datos, fijando los parámetros que se debían cumplir en el tratamiento de estos. Señalaba principalmente que "los datos personales debían ser tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, adecuados, pertinentes y no excesivos, exactos y, cuando sea necesario, actualizados, y deberán conservarse durante un período no superior al necesario y solo para los fines para los que fueron recogidos. Continuando en su artículo séptimo con aquellos criterios fundamentales y necesarios para que el tratamiento de datos pudiera ser considerado lícito.

En sus artículos doce y catorce establecía ciertos derechos que podía hacer valer el titular de datos personales respecto del responsable del tratamiento, a saber: a) el derecho a obtener información, como por ejemplo, saber la finalidad del tratamiento de sus datos o a quienes serán comunicados estos, entre otros; b) el derecho de acceso del interesado a los datos y finalmente; c) el derecho a oponerse al tratamiento de los datos cuando este no se ajuste a las disposiciones de la directiva.

Para hacer efectiva la correcta aplicación de las disposiciones normativas, la directiva disponía la existencia de una autoridad de control a la cual se le deberían notificar con anterioridad al tratamiento de datos la iniciación de dicha actividad. Luego esta entidad debía realizar una inspección al tratamiento de datos verificando la existencia de posibles riesgos que afecten los derechos y libertades de los interesados, y finalmente, una vez transcurrido lo anterior podía autorizar la publicidad del tratamiento de datos. Una vez que la autoridad haya sido notificada de dichos tratamientos deberá llevar un registro de ellos.

1.5 Nuevo Reglamento de Protección de Datos (Reglamento (UE) 2016/679)

Como mencionamos anteriormente, la Directiva 95/46 entra en vigencia en el año 1995, y debido al creciente avance tecnológico y, especialmente luego del mediático caso de Google contra la AEPD y Costeja, se hacía necesaria una normativa que se adecuara a la situación actual, es por esto que como señala Mayor (2016) "en el seno de la Unión Europea se empieza a considerar la necesidad de establecer un marco más sólido y coherente en materia de protección de datos en la UE, que evite la excesiva fragmentación en la aplicación de la protección de datos de carácter personal en el ámbito de la Unión Europea, y que fortalezca la seguridad jurídica de los ciudadanos europeos, operadores económicos y las autoridades públicas", razón por la cual el 27 de enero de 2012 se creó una propuesta de reglamento, la que luego de ser revisada y modificada derivó finalmente en el proyecto de reforma del Reglamento Europeo (UE) 2016/679 de Protección de Datos, aprobado el 12 de marzo de 2014 por el Parlamento Europeo, cuya publicación en el diario oficial de la Unión Europea se realizó el 4 de mayo de 2016, fijándose un plazo a los miembros de la Unión Europea para adecuar sus legislaciones a dicho reglamento, estableciendo como límite el 25 de mayo de 2018, fecha en la cual se deroga expresamente la Directiva 95/46/CE.

Este nuevo reglamento tiene como principal objetivo "regular las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos, así como la protección de los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. También se contempla como principio programático que la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales".

Este Reglamento General de Protección de Datos Personales (desde ahora también RGPDP) introduce varias novedades en cuanto a la regulación existente en materia de tratamiento y protección de datos personales. En primer lugar, al ser un reglamento y no una directiva como la Directiva 95/46/CE, es de aplicación directa en el derecho interno de los Estados de la Unión Europea por lo que nadie puede evadir su cumplimiento.

Sin lugar a duda una de las grandes novedades de este nuevo reglamento es el establecimiento explícito del derecho al olvido o también conocido como derecho de supresión, ya que no existía propiamente como tal, sino más bien había surgido y sido reconocido mediante interpretación jurisprudencial en el caso de Google contra la AEPD y Costeja, y otros casos más, sin existir regulación expresa en la Directiva 45/96 ni en ningún otro cuerpo normativo. El RGPDP lo regula en su artículo 17, señalando

que *"El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:*

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

Como podemos apreciar este reglamento establece aquellos casos en que es procedente el ejercicio del derecho al olvido por parte de los interesados. Claramente al no ser un derecho absoluto el derecho al olvido presenta ciertas excepciones frente a las cuales no tendrá cabida, dichas excepciones se regulan en este mismo artículo en su apartado tercero, donde señala que no podrá hacerse valer el derecho de supresión cuando el tratamiento de datos sea necesario: *"a) para ejercer el derecho a la libertad de expresión e información; b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3; d) con fines de archivo*

en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o; *e) para la formulación, el ejercicio o la defensa de reclamaciones*"

Junto con la introducción del derecho al olvido, este reglamento también viene a configurar un nuevo derecho: el de portabilidad, el cual consistente principalmente en la posibilidad que tienen las personas que consintieron en el tratamiento de sus datos personales para solicitar que el responsable actual de los mismo deje de realizarlo y traspase todos los datos correspondientes de esa persona a un nuevo responsable o gestor de tratamiento de datos, siempre y cuando se trate de un tratamiento automatizado.

A modo de resumen entonces, con este nuevo reglamento las personas quedan amparadas por los siguientes derechos: 1. Transparencia (art. 12); 2. Información (arts. 13 a 14); 3. Acceso (art. 15); 4. Rectificación (Art. 16); 5. Supresión o Derecho al Olvido (art. 17); 6. Limitación del tratamiento (art. 18); 7. Portabilidad de datos (art. 20) y; 8. Oposición (art. 21).

Además de lo anterior el RGPDP introduce otras modificaciones importantes relativas principalmente con el tratamiento y tráfico de los datos, una de ellas dice relación con el establecimiento explícito de los principios aplicables a la protección de datos (artículo 5 RGPDP) como, por ejemplo, el principio de transparencia, así como también el principio de responsabilidad. Este último tiene estrecha relación con el ámbito probatorio, ya que establece que la carga de probar que el tratamiento de datos se realiza de forma lícita y correcta corresponde al responsable de este y no a la víctima. A su vez, y vinculado con el tema probatorio, esta nueva normativa viene a regular el consentimiento, estableciendo expresamente los requisitos que debe cumplir este para que sea considerado válido, y pasa a señalar en su artículo 7 número 1 que "el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales", ratificando que la carga de la prueba recae en el responsable del tratamiento y no así en el afectado o titular de los datos.

Otra de las novedades es la introducción de nuevas categorías especiales de datos personales (artículo 9 RGPDP) correspondientes a aquellos "datos genéticos y los datos biométricos, cuyo tratamiento, en consecuencia, pasa a estar prohibido, con carácter general, en este caso siempre que se lleve a cabo con el fin de identificar de forma única una persona".

Se establece, también, en su artículo 30, la obligación a los responsables del tratamiento de datos de llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Así como

introduce la obligación de notificar a la autoridad de control la existencia de una violación de la seguridad de los datos personales, y su correspondiente comunicación a los interesados (artículos 33 Y 34 RGPDP).

Otra de los aspectos relevantes que introduce esta normativa es la creación del comité europeo de protección de datos (artículos 68-70 RGPD), órgano independiente conformado por "representantes de las autoridades de control de cada uno de los estados miembros, así como por el Supervisor Europeo de Protección de Datos y será responsable, entre otras cosas, de garantizar la aplicación coherente del reglamento, asesorar a la Comisión sobre toda cuestión relativa a la protección de datos personales en la Unión, emitir directrices y recomendaciones de buenas prácticas, o ser responsable de la acreditación de los organismos de certificación así como de su revisión periódica". También se introduce un sistema de ventanilla única (artículos 60-67 RGPDP) consistente en que aquellos responsables de tratamiento de datos que se encuentren establecidos en diversos países miembros, o bien, encontrándose en uno solo de ellos pero que realicen un tratamiento de datos que afecte a varios ciudadanos de distintos países miembros, tengan a una única autoridad de protección de datos como interlocutora.

Así mismo cabe destacar que modifica las sanciones y multas aplicables a aquellos responsables de tratamientos de datos que incumplan con la normativa (artículos 82-84 RGPDP), agravando las multas sancionatorias, además, establece la posibilidad de que la persona afectada con el tratamiento de datos inadecuado sea indemnizada directamente por los perjuicios causados, hecho que no ocurrían con las regulaciones preexistentes, significando un gran avance en materia de reparación a las víctimas.

1.6 Principios del Derecho al Olvido.

Antes de que se creara el nuevo Reglamento General de Protección de Datos Personales (RGPDP) no existía una legislación adecuada y concreta que regulara el Derecho al Olvido como tal, sin embargo, esta nueva normativa viene a regularlo expresamente en su artículo 17, y podemos extraer ciertas directrices o principios rectores que ayudan a la configuración de este derecho y a su correcta aplicación.

Uno de los principios rectores del derecho al olvido es el de finalidad, este se desprende del artículo 17 apartado 1 letra a), el cual señala que el interesado tendrá derecho a solicitar la supresión del tratamiento de sus datos personales cuando "ya no sean necesarios en relación con los fines para los que fueron recogidos o (sean) tratados de otro modo". Este principio entonces, consiste en que los datos tienen una cierta fecha de expiración o vencimiento, es decir, que al momento en que dejan de ser actuales o pertinentes, estos se vuelven automáticamente obsoletos, por lo que no habría razón alguna en su

mantención y debe procederse al retiro de los mismos de aquellos sitios que realizaron dicho tratamiento. Por ejemplo, en el caso de Costejas, al aplicar dicho principio, la página del diario que publicó la noticia referente a su persona debió haber procedido de forma inmediata a la eliminación de ella, así estos datos de carácter personal no hubieran seguido apareciendo en los resultados arrojados por los motores de búsquedas, desapareciendo completamente de la red, sin necesidad de recurrir a todas las instancias posteriores para amparar su derecho a honra y privacidad.

El consensualismo es otro de los principios que se extraen del reglamento, se desprende del artículo 6 apartado 1 letra a), que señala que el tratamiento de datos es lícito cuando "el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos", y por otro lado tenemos el artículo 17 apartado 1 letra b), relativo al derecho al olvido, el cual estipula que este puede tener aplicación cuando "el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico".

Como podemos apreciar, la voluntad del interesado cobra vital relevancia tanto para realizar un tratamiento de sus datos personales, como a su vez para retractarse y solicitar la eliminación o supresión de estos.

1.7 Excepciones del Derecho al Olvido

Como mencionamos anteriormente una de las características del Derecho al Olvido es que este no es un derecho absoluto y no se aplica erga omnes, sino que se encuentra sujeto a ciertas limitaciones o excepciones en su aplicación, debido a que una primacía de este podría terminar socavando otros derechos considerados relevantes para la sociedad.

Doctrinariamente hablando dichas excepciones o límites que se presentan en el Derecho al Olvido las podríamos agrupar de la siguiente manera:

a) Comunitarias: este tipo de excepciones atienden al interés público o común de la sociedad, señalando que aquellos datos o tratamiento de estos que se realicen con estos fines no podrán ser objeto del derecho al olvido, por lo que se debe proceder a su conservación a pesar de que el titular de los datos se oponga a ello.

Un ejemplo de lo anterior podría ser el registro que se lleva de los antecedentes penales de las personas, como es el caso de los registros de violadores o abusadores, el cual busca evitar que aquellas personas condenadas no se vinculen con menores de edad, solicitándole dicho certificado de antecedentes al momento de trabajar en escuelas, transporte escolar, etc., resguardando así la seguridad de los menores. Otro ejemplo atingente a este tipo de excepciones es aquel tratamiento o registro de información relacionada con la actividad pública o el ejercicio de esta por parte los funcionarios públicos. Los ministerios u otros organismos públicos deben rendir cuentas respecto de los sueldos que ganan quienes pertenecen a dichas organizaciones, para así transparentar su labor pública. Claramente esta información representa valor para la sociedad y es de interés público, ya que es importante conocer cómo los funcionarios y las entidades encargadas de gobernar realizan sus gestiones, y ver que estas sean correctas, para así evitar la malversación de fondos, el cometimiento de arbitrariedades, entre otras situaciones.

Este tipo de excepción se ve reflejada en el artículo 17 apartado 3, letra b del RGPDP, al establecer que no aplicará el derecho a suprimir el tratamiento de datos cuando este sea necesario "para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable".

b) De archivo: son aquellas en que los datos y la información son relevantes a nivel histórico, es decir, marcan un hito importante en el desarrollo de la historia, por lo que se debe guardar registro de ellos. Un ejemplo son aquellos registros que contienen datos personales llevados por las bibliotecas o los archivos nacionales, donde existen registros relacionados a la historia, ya sea universal o de cada país, los cuales no son susceptibles de ser suprimidos. Así lo estipula el artículo 17 apartado 3 letra d) del RGPDP al establecer que el tratamiento de datos que se realicen con "fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento", este no podrá ser eliminado.

c) Paternalistas: son aquellas en que se mantiene el registro de datos personales de un individuo en virtud de su propio interés, ya que, en caso de permitir la eliminación de esa información esto causaría perjuicios en la misma persona o interesado que pueda pretender borrarlos. Un ejemplo muy claro de ello es la necesidad de mantener un registro o historial clínico de los pacientes, ya que en ellos constan los antecedentes médicos y las enfermedades que padece una persona. Datos que ayudarían en caso de que esta tenga un accidente o recaiga nuevamente en

una enfermedad, pues si no se contara con ellos, no se podría saber a qué son propensos o si son alérgicos a algún medicamento, etc. Así se refleja también este tipo o clase de excepciones en el artículo 17 apartado 3 letra c) del RGPDP, que establece la prohibición de solicitar la eliminación de aquel tratamiento de datos realizado "por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3".

d) Administrativas o económicas: estas excepciones hacen referencia a aquella información que resulta fundamental para el funcionamiento institucional de un Estado. Un ejemplo de esto sería el registro de impuestos que se llevan a cabo en diversos países, pues como bien sabemos, estos son parte importante de los ingresos que reciben y, por consiguiente, ayudan a la economía del país. Es por esto que el tratamiento de los datos personales de aquellas personas que pagan sus impuestos no podría ser sometidos al derecho de supresión por parte de algún interesado, ya que son considerados necesarios para el funcionamiento de cada Estado. Otro ejemplo es el registro de las votaciones que se llevan en cada país, evidentemente el tratamiento de los datos personales de los votantes habilitados para sufragar en cada Estado y su correspondiente conservación es de vital importancia para mantener las diversas instituciones de los países democráticos, pues la alteración o eliminación de dichos registros podría derivar en un caos de los gobiernos, que se produciría por las alteraciones de las votaciones, habiendo personas que votarían más de una vez, suplantación de votantes que ya han fallecido, etc., incidiendo en la validez de las elecciones generando con esto una inestabilidad institucional.

e) Legales: son aquellas excepciones que se dan cuando una ley particular ordena la conservación de determinada información que contenga datos personales. Este tipo de excepción es recogida por el RGPDP en su artículo17 apartado 3 letra b), al señalar que no podrá solicitarse el derecho al olvido respecto de aquel registro de datos necesario "para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento".

f) De seguridad: este grupo de excepciones se refieren principalmente a aquel tratamiento de datos relativos a la seguridad de un Estado y sus habitantes. Un ejemplo de esto sería la conservación que se realiza de los datos personales de aquellas personas involucradas en una investigación criminal.

g) Voluntarias: estas excepciones son un reflejo del principio de consensualismo, y se refieren principalmente a aquellas en que la misma persona respecto de la cual se realiza un tratamiento

de sus datos personales, desea conservar dicha información, ya que el consentimiento es, por regla general, requisito para tratar datos de carácter personal.

En las diversas legislaciones que regulan la protección de datos o el Derecho al Olvido en específico, sean normativas individuales y propias de cada país, o bien, se trate de legislaciones internacionales para diversas asociaciones de países, podremos apreciar la existencia de diversas excepciones concretas al derecho al olvido o de supresión que perfectamente pueden encasillarse en alguna de las clasificaciones anteriormente expuestas.

Capítulo 2: Derecho al Olvido en Chile

2.1 Situación Actual

Como pudimos apreciar en el capítulo anterior, el derecho al olvido se encuentra en plena formación y desarrollo, creándose legislaciones y marcos regulatorios posteriores a la realidad y los avances tecnológicos a los cuales nos hemos visto sometidos de forma exponencial en las últimas décadas.

Hoy en día la situación particular de nuestro país frente al derecho al olvido es escasa y vaga. No existe en nuestra legislación una ley que regule de manera efectiva la protección de los datos personales, ni mucho menos se contempla el derecho al olvido como un derecho que busque amparar a los ciudadanos frente al tratamiento de sus datos de carácter personal. Es más, hasta hace muy poco la protección de los datos personales no era considerada como uno de los derechos básicos y fundamentales que asegura nuestra Constitución a todas las personas, de hecho, lo más próximo a su regulación y protección era la ley 19.628 sobre "PROTECCION DE DATOS DE CARACTER PERSONAL" (LPDP), la que no está exenta de críticas debido a lo anacrónica de la misma, pues es una ley que entra en vigor en el año 1999.

Son exiguos los casos en que nuestros tribunales hayan tenido que conocer y dirimir acerca de la aplicación del derecho al olvido, sin embargo, es pertinente señalar que el primer caso en el que se aplica el derecho al olvido ocurrió en el año 2011, en que la Excelentísima Corte Suprema ordenó dar de baja de Facebook unas fotografías que fueron publicadas en un grupo de la mencionada red social en las que aparecían retratados menores de edad mientras se producían saqueos luego del trágico terremoto del año 2010. El máximo tribunal nacional ordenó esto aduciendo en su fallo que la imagen atentaba contra la integridad física y psicológica de dos menores y que, además, contravenía la Convención sobre los Derechos del Niño. Junto con lo anterior fundamentó que existía un actuar ilegal y arbitrario por parte de los recurridos, y que era sumamente necesario otorgar protección a la imagen e integridad física y psicológica de los menores, las cuales deben ser priorizadas frente a la actitud que se les reprocha, así como el hecho de que los recurridos fomentaban a través de sus comentarios en la foto, injurias y amenazas por parte de terceros, entre otros argumentos.

La pertinencia de traer en comento el presente caso se debe a que se recoge de manera tenue el derecho al olvido. Claramente el objetivo principal que implica este derecho no se cumple abiertamente porque solo obliga a quienes subieron la fotografía a la pertinente eliminación de esta y de los comentarios hacia ella, pero nada se señala respecto a los terceros que pudieron haber descargado dicha fotografía de la red social o haberla compartido en otros grupos o páginas web, además, es necesario señalar que el derecho

al olvido no es el fin último del fallo, si no que más bien se ordenó la eliminación de las fotografías con el objetivo de dar protección a los derechos del niño que habían sido vulnerados con dicha publicación.

Este es someramente el panorama actual en nuestro país relativo a la regulación de los datos personales y del derecho al olvido. A continuación, se procederá al análisis de la ley 19.628 de forma extensa para poder conocer con más detalles como se tratan los datos personales de los individuos en Chile. También hablaremos del proyecto de ley existente hoy en el congreso que busca mejorar las falencias en la actual normativa, así como también veremos ciertos casos que reflejen la visión actual que tienen nuestros tribunales al momento de aplicar el derecho al olvido.

2.2 Ley 19.628 "SOBRE PROTECCIÓN DE LA VIDA PRIVADA"

La ley 19.628, de ahora en adelante la Ley o LPDP, fue promulgada el 18 de agosto de 1999, con el objetivo de regular y proteger el tratamiento de los datos de carácter personal que llevan a cabo los registros o bancos de datos, sean estos realizados por organismos públicos o por entes particulares, sea que se trate de un tratamiento de carácter automatizado o manual. Violler (2019) indica, "Aunque se trata de una de las primeras leyes de protección de datos personales en América Latina, este cuerpo legal fue considerado insuficiente para proteger a los individuos del tratamiento de sus datos personales por parte de terceros, incluso, en la discusión legislativa previa a su tramitación".

La ley cuenta con 24 artículos permanentes y 3 artículos transitorios, se divide en 7 títulos, a saber:

- Título preliminar: Disposiciones generales (artículos 1-3).
- Título I: De la utilización de datos personales (artículo 4-11).
- Título II: De los derechos de los titulares de datos (artículos 12-16).
- Título III: De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial (artículos 17-19).
- Título IV: Del tratamiento de datos por los organismos públicos (artículos 20 a 22).
- Título V: De la responsabilidad por las infracciones a esta ley (artículo 23).
- Título Final, que modifica el Código Sanitario (artículo 24).

A continuación, desglosaremos algunos de los temas que se consideran más relevantes en materia de protección de datos tratados por esta legislación.

2.2.1 Regla del consentimiento, nociones y características.

Según el artículo 4 de la ley 19.628 en su inciso primero señala que "el tratamiento de los datos personales solo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello".

Como podemos apreciar, el consentimiento de las personas en el tratamiento de los datos es una de las fuentes que lo permite y le otorga legalidad, por lo que analizar cómo debe ser este, sus requisitos y las características que reviste resultan relevantes en esta materia.

Si bien la ley hace referencia al consentimiento como uno de los presupuestos para poder realizar un tratamiento de datos, no nos da un concepto o una definición acabada de esta autorización consentida, solamente se limita a señalar que la persona que presta su consentimiento debe estar informada respecto a la finalidad o propósito de la recolección de sus datos y que su consentimiento debe ser constatado por escrito.

Como la ley es escueta en cuanto a la forma en que se debe entregar este consentimiento, recurrimos al derecho comparado, donde encontramos que la autorización consentida sucintamente debe recoger las siguientes características:

a) Manifestado: el consentimiento debe ser de forma expresa, cerrando toda posibilidad de manifestación tacita o presunta. Con respecto a su oportunidad no se especifica en la ley, sin embargo, se infiere que debiera ser antes del procesamiento respectivo de los datos ya que la regla no puede ser la libertad de estos y después una ratificación por parte del titular.

b) Libre: esta característica atiende en general a que el consentimiento debe estar exento de vicios y debe ser prestado de forma autónoma y espontánea. La LPDP no hace referencia a esta característica, pero podríamos extraerlo de las reglas generales que establece nuestro código civil en materia de manifestación de voluntad y de consentimiento.

c) Debe constar por escrito: Esta característica o requisito si se encuentra regulado expresamente por la ley 19.628, como señalábamos anteriormente, en su artículo 4.

d) Específico: esta característica del consentimiento está íntimamente ligada a uno de los principios que rigen el tratamiento de datos, el denominado principio de finalidad que detallaremos más adelante. Este requisito lo encontramos o extraemos del mismo artículo 4 de la Ley, ya que señala que, al momento de prestarse el consentimiento por la persona, esta debe ser informada respecto a la finalidad por la cual se van a recoger sus datos, prestándose entonces dicho consentimiento solo para realizar el tratamiento de sus datos con ese propósito específicamente y no extendiéndose a ningún otro tratamiento.

e) Informado: esta característica tiene relación con la anterior, pues se exige expresamente en la LPDP que la persona antes de prestar el consentimiento debe ser informada con respecto al fin de la utilización de sus datos.

Si bien el consentimiento para autorizar el tratamiento de datos es la regla general, es el mismo artículo 4 quien en sus incisos posteriores establece excepciones en las cuales se puede realizar dicho tratamiento de datos a pesar de no contar con la aquiescencia del titular de los mismos. Señala este artículo en su inciso quinto lo siguiente: "No requiere autorización el tratamiento de datos personales que (1) provengan o que se recolecten de fuentes accesibles al público, (2) cuando sean de carácter económico, financiero, bancario o comercial, (3) se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o (4) sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios", añadiendo en su inciso final una quinta excepción relativa al "tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquellos".

Como podemos apreciar, solo en este artículo encontramos cinco excepciones en cuanto a la exigencia del consentimiento del titular de los datos como requisito para su correspondiente tratamiento, por lo que es a lo menos cuestionable señalar que el consentimiento es la regla general en dicha materia, ya que la existencia de tantas de aquellas termina por coartar la real y efectiva importancia de la aquiescencia de los titulares. Y no son las únicas excepciones que establece la ley, ya que en su artículo 20 nos encontramos con casos en los que se prescinde del consentimiento de titular, señalando que (6) "el tratamiento de datos personales por parte de un organismo público solo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular". Además, es necesario señalar que tampoco será necesario (7) "cuando el tratamiento de datos personales se efectúe para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares (artículo 10)". (Jervis, 2005).

Sin lugar a dudas, de todas las excepciones mencionadas anteriormente, la que genera mayor controversia es la relativa a los datos recolectados o provenientes de fuentes accesibles al público, esto debido a que es una excepción bastante amplia pues la ley realiza una definición paupérrima de lo que debemos entender por dichas fuentes, señalando en su artículo 2 letra i) que estas corresponden a "los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes", lo que conlleva a que, en palabras de Viollier (2019) "sean los titulares quienes se ven privados de la protección que la ley les debería brindar. Países con un estándar más alto de protección de datos personales, como España, han optado por definir de forma más acotada qué se debe entender por fuente accesible al público, e incluso establecer un catálogo taxativo de las fuentes que pueden considerarse dentro de esa categoría", soluciones que nuestros legisladores deberían tener en consideración a la hora de regular este asunto.

A su vez, así como se puede prestar el consentimiento para la recolección o tratamiento de los datos relativos a una persona, también esta puede revocar el consentimiento dado, acto que tendrá plena validez siempre y cuando se realice de forma escrita, pero que no producirá efectos de manera retroactiva, es decir, no rige para el tiempo intermedio entre la autorización y la revocación. Y si la información hubiera sido compartida con terceros, se les debe comunicar dicha cancelación o eliminación de datos cuando esto fuere posible, y en caso de que no se pudieren identificar a estos terceros a quienes se les compartieron los datos, se debe dejar un aviso general para que se enteren quienes usen la información del banco de datos respectivo.

Referente a esto Jervis (2005), también indica "Sin perjuicio de lo señalado, reconocemos que puede argüirse que al no estar regulada en nuestra legislación la figura de la autorización del titular de los datos en la cesión de ellos y al ser legítimo el tratamiento de datos efectuado con antelación a la revocación –incluida la cesión- … este tercero podría legítimamente seguir tratando los datos personales cedidos no obstante la revocación".

2.2.2 Tipos de datos consagrados en la Ley 19.628.

La ley 19.628 en su título preliminar realiza diversas definiciones, como ejemplo señala en su artículo 2 letra a) que el almacenamiento de datos corresponde a "la conservación o custodia de datos en un registro o banco de datos", a su vez define este último como aquel "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". En cuanto

al ámbito de aplicación subjetivo de la ley, nos encontramos con que existen dos tipos de sujeto. En primer lugar, tenemos al responsable del registro o banco de datos, definidos en el artículo 2 letra n) como la "persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal". En segundo lugar, tenemos a los titulares de los datos, señalando en el mismo artículo letra ñ) que corresponden a aquella "persona natural a la que se refieren los datos de carácter personal". Finalmente, parece relevante señalar la definición que realiza en el mismo artículo letra o) respecto de lo que se entiende por tratamiento de datos, siendo "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma".

Como bien sabemos el objetivo principal de esta ley es regular el tratamiento que se realiza de los datos personales en nuestro país. Por eso nos parece necesario mencionar las clasificaciones de datos que encontramos en este cuerpo legal:

- Datos personales: definidos en su artículo 2 letra f) como aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

- Datos sensibles: son definidos como 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. Cabe mencionar que respecto a este tipo de datos personales la ley prohíbe expresamente su tratamiento en su artículo 10, salvo ciertas excepciones, y que son cuando (1) la ley lo autorice, (2) exista consentimiento del titular o (3) sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

- Datos caducos: se entiende por este, aquel dato que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.

- Datos estadísticos: es aquel dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable. De acuerdo con esta misma definición se señala entonces que esta categoría de datos queda fuera de los tipos de datos que regula la normativa en cuestión.

2.2.3 Principios consagrados en la Ley 19.628

En materia jurídica los principios en que se basan las legislaciones son aspectos fundamentales para su creación y posterior aplicación, y en palabras de Alexy (2008) podríamos decir que "los principios son normas que ordenan que algo sea realizado en la mayor medida posible, de acuerdo con las posibilidades fácticas y jurídicas. Por ello, los principios son mandatos de optimización. Como tales, se caracterizan porque pueden ser cumplidos en diferentes grados y porque la medida de cumplimiento ordenada depende no sólo de las posibilidades fácticas, sino también de las posibilidades jurídicas. Las posibilidades jurídicas se determinan mediante reglas y, sobre todo, mediante principios que juegan en sentido contrario".

En la ley 19.628 sobre protección de datos personales podemos encontrar ciertos principios rectores que rigen en esta materia, dentro de los más importantes o los más destacados encontramos los siguientes:

a) Principio de libertad en el tratamiento de datos: estipulado en la ley, específicamente en su artículo primero inciso segundo, señalando que "toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico". Como podemos ver la ley faculta a cualquier persona para realizar tratamiento de datos personales, siendo la regla general el libre albedrío para gestionar un banco de datos, siempre y cuando se realice de acuerdo con la normativa vigente.

b) Principio de finalidad: Se encuentra consagrado en el artículo 9 de la ley sobre protección de datos personales, y consiste principalmente en que estos deben utilizarse solo para los fines para los cuales hubieren sido recolectados. Se encuentra íntimamente ligado con el principio del consensualismo y el derecho de información que tiene el titular de los datos, ya que, como mencionábamos con anterioridad, la persona que presta el consentimiento para el tratamiento de sus datos debe estar informada del propósito con el que se realiza, y por ende no puede el responsable de los bancos de datos continuar con dicho tratamiento si el propósito o finalidad del mismo cambia, pues no se extiende el consentimiento del titular. Sin embargo, este principio de finalidad tiene una excepción, ya que en caso de que provengan o se hayan recolectado de fuentes accesibles al público, estos pueden utilizarse aún para fines que no se tuvieron al momento de su recolección. El artículo 9 ley 19628, señala "Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados salvo que provengan o se hayan recolectado de fuentes accesibles al público".

c) El principio de inalienabilidad: este principio consiste o significa que los derechos otorgados por la presente ley a los titulares de los datos no se pueden enajenar, es decir, el dominio de estos no se puede

traspasar o transmitir de un individuo a otro, por lo tanto, no pueden venderse o cederse de manera legal. Este principio se encuentra consagrado en el artículo 13 de la Ley, "El derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención"

d) El principio de gratuidad: consiste en el hecho de que los titulares de los datos personales al momento de ejercer sus derechos se encuentran exentos de pago alguno, es decir, no deben cancelar ningún monto cuando soliciten de los responsables del registro o del banco de datos el acceso a la información, la modificación o su eliminación, o cuando interpongan la acción de habeas data judicialmente en caso de negárseles sus solicitudes por parte de los responsables del tratamiento de datos, el artículo 12 inciso quinto de la Ley, señala que "la información, modificación o eliminación de los datos serán absolutamente gratuitas".

Sin embargo, la Ley omite el derecho de bloqueo en la norma, por lo que dicho derecho no está amparado por el principio de la gratuidad, razón por la cual podría estar sujeto a algún tipo de cobro, que en todo caso, nunca podrá ser de tal entidad que imposibilite su ejercicio, es decir, debe ser un cobro racional y proporcional. Además, en este mismo artículo en su parte final, se señala que la gratuidad no solo se establece para el correcto ejercicio de los derechos, sino que además se extiende a las copias que deben entregar los responsables del registro o de los bancos de datos cuando se realice alguna modificación por solicitud de acceso a la información, modificación o eliminación de los datos personales por parte de sus titulares. Y no solo es gratis la primera vez que se ejerzan los derechos mencionados, sino que también deberán entregarse copias gratuitas del registro actualizado si se efectuasen nuevas modificaciones o eliminaciones de datos, sin perjuicio de que deben haber transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de los derechos aludidos y que además este se ejerza personalmente. Art. 12 inc. 5° Ley 19.628. "Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que haya transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita sólo podrá ejercerse personalmente".

e) El principio de calidad de los datos: este principio se encuentra consagrado en el artículo 6 de la Ley de la siguiente forma: "los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado. Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos. Se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación", y agrega en su inciso final que "El responsable del banco de datos personales procederá a la eliminación, modificación o bloqueo de los datos, en su caso, sin necesidad de requerimiento del

titular". Es en este último inciso donde encontramos consagrado el principio de calidad de los datos, y se refiere a que cada vez que los datos personales revistan alguna de las características que se mencionan en los incisos precedentes, es decir, sean datos en que su almacenamiento carezca de fundamento legal, sean caducos, inexactos, erróneos, equívocos, incompletos, su exactitud no pueda ser establecida o cuya vigencia sea dudosa, los responsables de la recaudación o de los bancos de datos, sin que necesariamente el titular accione y ejerza dichos derechos, deberán proceder a la modificación, eliminación o bloqueo inmediato de aquellos datos, es decir, están obligados por ley a proceder de esa manera, pues de lo contrario estarían incurriendo en un acto contrario a la ley.

f) Principio de responsabilidad: consagrada en el artículo 11 de la ley 19.628, estableciendo que el encargado de los registros o bases donde se almacenen datos personales deberá, con posterioridad a su recolección, cuidar de ellos con la debida diligencia, haciéndose responsable de los daños que dicho tratamiento pueda ocasionar a los titulares de los datos personales.

Son estos algunos de los principios más importantes que rigen en la protección de los datos personales y de la privacidad de las personas.

2.2.4 Derechos protegidos o tutelados por la Ley 19.628.

El objetivo principal de la ley 19.628 es regular el tratamiento de los datos de carácter personal que se lleven a cabo en registros o bancos de datos, ya sea por organismos públicos o por particulares. La regla general es la libertad para realizar dicho tratamiento, ya que cualquier persona puede llevarlo a cabo siempre y cuando lo haga bajo los parámetros legales. Es por lo anterior que la ley sobre protección de datos personales, como una forma de contrarrestar este principio, establece en su título II, cuatro derechos específicos que el titular de los datos puede ejercer en determinados casos. Cabe señalar que la propia ley establece que dichos titulares sólo corresponden a personas naturales, es decir, que aquellas personas jurídicas que se puedan ver afectados por la recolección o tratamiento de sus datos quedan fuera de esta protección.

Los derechos amparados para los titulares de datos en la ley 19.628 son los siguientes:

a) El Derecho de Acceso a la información: este derecho se encuentra en el artículo 12 inciso 1 de la respectiva ley, y consiste principalmente en que el titular de los datos personales puede exigir de los responsables de los bancos de datos, sean estos públicos o privados, la entrega de toda la información que se tenga respecto de ella, así como también su procedencia o lugar de obtención, a quienes fue

compartida dicha información, individualizando a las personas u organismos que tuvieron acceso a ella y la comunicación de la finalidad por la cual se almacenan sus datos personales.

b) El Derecho de Modificación: se encuentra establecido en el artículo 12 inciso 2 de la ley, y consiste en la alteración o cambio de aquella información errónea, equívoca, falsa o incompleta que se tenga respecto de una persona. Dichas características deberán ser acreditada por el titular.

c) El Derecho de Eliminación: se encuentra determinado en el artículo 12 inciso 3 de la ley, y consiste en la destrucción de aquella información extemporánea, que ha perdido actualidad o aquella que carezca de fundamento legal para su conservación. En la misma normativa en su artículo 2 letra h) encontramos la definición de eliminación o cancelación de datos, siendo esta "la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello". Este derecho de cancelación es lo más próximo o similar al derecho al olvido en nuestra legislación.

d) El Derecho de Bloqueo: por su parte este derecho se encuentra definido en el artículo 2 letra b), y señala que consiste en la "suspensión temporal de cualquiera de las operaciones de tratamientos 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 corresponde la cancelación.

Respecto de los últimos dos derechos mencionados (derecho de eliminación y derecho de bloqueo) la ley, en su artículo 12 inciso 4, agrega que podrán ejercerse también respecto de aquellos datos personales que una persona haya proporcionado voluntariamente o si ellos se usaren para comunicaciones comerciales y el titular no desee continuar figurando en el registro respectivo, produciéndose de modo definitivo o temporal.

Como podemos apreciar la ley 19.628 es una de las más importantes que existen en materia de regulación relativas al tratamiento y recolección de datos personales, así como de protección a la vida privada en Chile, siendo la legislación más homologa que existe hoy en día al derecho al olvido. Esto porque se establece en ella uno de los derechos más importantes que se les otorgan a los titulares de los datos personales, aquel consistente en la eliminación de aquellos datos respecto de los cuales su conservación carezca de fundamento legal o cuando estuvieren estos caducos, es decir, existe una especie de derecho al olvido en nuestra legislación, pero es bastante limitada debido a las excepciones de eliminación, modificación y bloqueo que presenta el mismo cuerpo legal.

Estas limitaciones se encuentran en el artículo 15 de la Ley, el cual señala que no procederán las solicitudes de acceso a la información, eliminación, modificación y boqueo respecto de aquellos datos personales cuando ello:

- Impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido
- Afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias
- Afecte la seguridad de la Nación o el interés nacional
- Cuando se trate de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva. Sin embargo, esta limitación no se extiende al derecho de acceso a la información. (JERVIS, 2003)

Los derechos anteriormente vistos y analizados corresponden a aquellos derechos fundamentales que componen la columna vertebral relativa a la protección de los datos personales propiamente tal, sin embargo la ley concede tres derechos más a los titulares de datos personales: (i) uno de ellos consiste en el derecho de oposición, establecido en el artículo 3 inciso final de la Ley, que faculta al titular para oponerse a la utilización de sus datos personales cuando sean utilizados con fines de publicidad, investigación de mercado o encuestas de opinión; (ii) el segundo derecho, establecido en el artículo doce inciso cuarto, corresponde a la obligación de comunicación a aquellos terceros a quienes los responsables de los bancos de datos les han compartido datos personales, cuando estos últimos han sufrido eliminaciones o bloqueos; (iii) finalmente tenemos el derecho de copia, consagrado en el artículo doce inciso quinto, estableciendo este que cada vez que se ejerzan los derechos de modificación y eliminación, el titular de los datos tendrá derecho a que se le entregue una copia registro de los respectivos datos personales actualizado, es decir, con la transformación o destrucción correspondiente de aquellos datos que no correspondían. Dichas copias están afectas a gratuidad, es decir, no debe cancelarse monto de dinero alguno para obtenerlas. No obstante, este derecho a copia gratuita tiene una limitación, y es que para que sea gratuita deben haber transcurrido a lo menos seis meses desde que se ha realizado anteriormente el ejercicio de algunos de los derechos en cuestión.

Estos son los derechos que la Ley consagra respecto a la protección de la vida privada y consecuencialmente de los datos personales. El ejercicio de estos derechos se encuentra protegido o cautelado mediante la acción de habeas data que establece el artículo 16 de la Ley 19.628, la cual procederemos a explicar en el siguiente apartado.

2.2.5 Procedimiento de la acción de Habeas Data.

Como mencionamos anteriormente la acción de habeas data es una acción que puede ejercer el titular de los datos personales cuando vea conculcados en ciertas situaciones los derechos otorgados por la Ley

19.628, es decir, el derecho de acceso a la información, modificación, eliminación o bloqueo de la misma. Esta acción es de rango legal, ya que se encuentra consagrada en el articulado dieciséis de la citada normativa, a diferencia por ejemplo de la acción de habeas corpus (recurso de amparo), que se encuentra consagrado en la Constitución chilena y por lo tanto tiene rango constitucional. Este artículo 16 establece que "Si el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, que se encuentre de turno según las reglas correspondientes, solicitando amparo a los derechos consagrados en el artículo precedente" agregando en su inciso tercero que "En caso de que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional, la reclamación deberá deducirse ante la Corte Suprema"

Como podemos ver se dan tres presupuestos en los cuales procederá la acción de habeas data, y esto son:

a) En primer lugar, cuando exista silencio por parte de los responsables de los bancos de datos frente a las solicitudes de acceso a la información, modificación, eliminación o bloqueo que le hagan los titulares de los datos personales, cumplido el plazo de dos días que poseen para pronunciarse al respecto.

b) En segundo lugar, cuando existiese un rechazo a la solicitud de acceso, modificación, eliminación o bloqueo de la información de los datos de una persona, por parte de los responsables de los bancos de datos aludiendo o invocando a una causa diferente a la seguridad Nación o el interés nacional.

c) En tercer lugar, cuando existiese un rechazo a la solicitud de acceso, modificación, eliminación o bloqueo de la información de los datos de una persona, por parte de los responsables de los bancos de datos aludiendo o invocando como causa de ello a la seguridad Nación o el interés nacional.

Otras causales en las que procede la interposición de la acción de habeas data es por la infracción a los artículos 17 y 18 de la Ley 19.628, que regulan la forma y los plazos en que pueden comunicarse a terceros por los responsables de los registros o bancos de datos de carácter económico, financiero o comercial. (Art. 16 inc. 5°). Así como también procederá respecto de las infracciones no contempladas en los artículos 16 y 19. (Art. 23 inc. 2°), ésta última se refiere a la acción indemnizatoria que puede ejercer el titular de los datos que se haya visto perjudicada por el tratamiento indebido que se haya realizado de los mismos, la cual puede ser interpuesta conjuntamente con la reclamación.

En la ley no se establece un procedimiento único para interponer la acción de habeas data, sino que encontramos tres tipos de procedimientos, dependiendo de las hipótesis o supuestos en que ocurran infracciones a los derechos de los titulares de datos personales. A continuación, procederemos a la explicación de los procedimientos existentes en la ley para el ejercicio de la acción habeas data.

I. El procedimiento general: este procedimiento se encuentra reglamentado en el artículo dieciséis de la Ley, específicamente en sus incisos primero y segundo. Se aplica este procedimiento cuando el responsable de la recaudación o bando de datos no se pronunciare respecto de las solicitudes que realicen los titulares de los datos personales relativas al acceso a la información, su modificación, eliminación o bloqueo, en el plazo de dos días, o bien cuando se denegare dicha solicitud aludiendo causales que no corresponden a la seguridad de la Nación o al interés nacional. Solo cuando ocurran estos dos presupuestos procederá la aplicación del procedimiento general de reclamación.

En primer lugar, señala la Ley que en este procedimiento el juez competente para conocer de la interposición de la acción es el juez de letras en lo civil correspondiente al domicilio del responsable de la recaudación o del banco de datos, es decir se sigue la regla general que establece el Código Civil, el cual señala que el tribunal competente es aquel que corresponda al domicilio del demandado. Una vez determinado el tribunal competente para conocer del asunto el titular de los datos deberá solicitar el amparo a los derechos consagrados en el cuerpo normativo. En dicha reclamación el titular deberá señalar de forma clara la infracción cometida y los hechos que la configuran, como así también deberán acompañarse todos los medios de prueba que los acrediten, en su caso. La notificación de la reclamación se hará por cédula, y será dejada en el domicilio del responsable del banco de datos correspondiente, en la cual se concederá traslado para que éste último realice los descargos correspondientes dentro del plazo de quinto día hábil, los cuales deberán ir acompañados de los medios de prueba que pretenda hacer valer, o en caso de no poder presentarlos, solamente deberá ofrecerlos y explicar las circunstancias que le impiden su presentación en ese momento, caso en el cual el tribunal fijará una audiencia dentro de quinto día hábil a fin de recibir la prueba ofrecida. Claramente vemos que en este último punto se produce una inequidad de las partes, vulnerándose el principio de igualdad en el procedimiento, ya que se le concede al responsable del banco de datos dos oportunidades para presentar las pruebas correspondientes, mientras que al titular de los datos que se ve vulnerado la ley solamente le otorga una oportunidad, la cual una vez precluida, ya no podrá presentar sus pruebas con posterioridad.

La sentencia definitiva se dictará dentro de tercero día de vencido el plazo a que nos referimos anteriormente, sea que se hayan o no presentado descargos. Si el tribunal decretó una audiencia de

prueba, este plazo correrá una vez vencido el plazo fijado para ésta. Esta sentencia será notificada por cédula, en la misma forma en que se realiza la notificación de la reclamación interpuesta por el titular de los datos personales.

Dicha sentencia será susceptible del recurso de apelación, el cual se concederá en ambos efectos, y deberá recurrirse dentro del plazo de quinto día hábil, contados desde la notificación que se le realiza a la parte que lo entabla. Dicho recurso deberá contener los fundamentos de hecho y de derecho en que se funda y las peticiones concretas que se solicitan. Deducida la apelación, el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes. Sin embargo, podrá ordenar traer los autos en relación para oír a los abogados de las partes, para lo cual deberá agregar extraordinariamente la causa a la tabla respectiva de la misma sala. La resolución que se pronuncie respecto del recurso de apelación será susceptible del recurso de casación. Cabe señalar que, salvo la sentencia definitiva, todas las demás resoluciones se dictarán en única instancia y se notificarán por el estado diario.

II. El procedimiento especial: este procedimiento se aplica cuando el responsable de la recaudación de los datos o del banco de datos se negare frente a las solicitudes de los titulares de derechos para acceder, modificar, eliminar o bloquear la información que contenga sus datos personales, invocando como causal la seguridad de la Nación o el interés nacional. La acción de habeas data deberá interponerse, ya no frente al tribunal de letras en materia civil de turno correspondiente al domicilio del responsable del banco de datos, sino que debe interponerse directamente ante la Corte Suprema, quien solicitará un informe de la autoridad de que se trate por la vía que considere más rápida, fijándole un plazo determinado para su entrega, el cual una vez transcurrido, dará paso a que el máximo tribunal nacional resuelva en cuenta la controversia suscitada. No obstante, lo anterior podrá ordenar traer los autos en relación para oír a los abogados de las partes, procediendo a agregar la causa extraordinariamente a la tabla respectiva de la misma sala. Para lo cual el presidente del Tribunal dispondrá que la audiencia no sea pública. En caso de que se reciba prueba al respecto, se consignará en un cuaderno separado y reservado, que conservará ese carácter aún después de terminada la causa, si por sentencia ejecutoriada se denegare la solicitud del requirente.

III. El procedimiento sumario: este procedimiento tiene el carácter de ser residual, pues así se desprende del artículo 23, en donde se encuentra consagrado dicho procedimiento, el que señala que “las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. Por ejemplo, si el órgano público trata datos

fuera del ámbito de su competencia, o si el responsable de datos no cumple con la obligación de avisar a terceros que los datos han sido modificados o eliminados, etc. (JERVIS, 2003)

2.3 Críticas al Sistema político y jurídico chileno frente al derecho al olvido y la protección de los datos.

La ley 19.628 fue promulgada en el año 1999, es decir, es una ley que nace hace 20 años atrás, la cual ha sufrido escuetas modificaciones, las cuales no han sido de carácter sustancial, y es evidente que ha quedado obsoleta en cuanto a los grandes avances tecnológicos y a la importancia que han adquirido hoy en día el tratamiento de datos personales, es por lo mismo que a continuación se analizarán las principales falencias que encontramos en la misma ley, así como también en la legislación en general existente en nuestro país relativa a la privacidad y protección de los datos personales.

2.3.1 Errores que podemos atribuirles a la LPDP (errores en la redacción, reglas incompletas, ambiguas, contradictorias, vacíos legales entre otros)

Al momento de referirnos al consentimiento como requisito para realizar tratamiento de datos, nos encontramos con la falencia de que si bien se exige éste, la ley no específica o se refiere al momento en el cual se requiere dicha autorización por parte del titular de datos, por lo que deja abierto el debate a si el consentimiento finalmente se requiere antes de proceder al tratamiento de datos, o bien puede ser otorgado de forma posterior funcionando como una especie de ratificación. A su vez tampoco se refiere la ley a que este consentimiento debe ser libre y espontáneo, solamente se refiere a que debe constar por escrito, más nada dice respecto a la existencia de vicios que pudieran invalidar el consentimiento dado para la autorización del tratamiento de datos.

Además de lo anterior el consentimiento se ve bastante limitado por las excepciones que establece la ley en donde no es requerido y se puede proceder de todas formas al tratamiento de los datos personales, por lo que se debería proceder a derogar ciertas excepciones como por ejemplo el caso del marketing directo.

En lo que respecta a la cesión del tratamiento de los datos del titular hacia terceros la ley no exige autorización para la comunicación de los mismos. Claramente se produce una vulneración hacia el titular de los datos personales, pues éste al momento de prestar su consentimiento autoriza a cierta persona a

realizar dicho tratamiento, más no autoriza el traspaso a terceros. Esta vulneración no ocurre en el derecho comparado, ya que se exige consentimiento para poder traspasar los datos a un tercero por parte del responsable de la base de datos. Y la mayor consecuencia de esto es que el titular de los datos queda absolutamente desprotegido pues no puede solicitar no se le puede exigir a este tercero el cese del tratamiento en los casos en que sean indeterminados.

Otra de las críticas que podemos realizar a la ley es el hecho de que en ninguna parte distingue el tratamiento de datos correspondiente a adolescentes o menores de edad, quienes claramente deberían tener un estatuto diferenciado por su especial condición.

En materia de legitimación activa o pasiva del titular no se señala en la ley si aplica la figura de la representación para el ejercicio de los derechos otorgados. Al no existir claridad al respecto, se han señalado 2 posturas en la doctrina, en primer lugar, nos encontramos con aquellos que señalan que se tratan de derechos personalísimos y por ende no tendría cabida la representación. Por otro lado, nos encontramos con aquellos que señalan que si se debiese admitir la representación, apoyándose fundamentalmente en dos argumentos, el primero de ellos dice relación con el caso de los menores de edad o aquellos sujetos que se encuentren fuera del país, los cuales no podrían ejercer por sí mismo los derechos otorgados en la ley, requiriendo que otro actúe en su nombre. En segundo lugar, argumentan que en la generalidad de los actos jurídicos se admite la representación a través de mandato, por lo que no tendría por qué ser distinto para este caso, además la LPDP señala que el único derecho que es de ejercicio personal es el de copia gratuita, por lo cual a contrario sensu se entendería que todo el resto admitiría representación teóricamente.

Otra crítica que se le realiza a la ley es respecto a la gratuidad de los derechos que otorga al titular de los datos, ya que como mencionamos con anterioridad el ejercicio de los mismo son de carácter gratuito, sin embargo, no todos se encuentran mencionados en la lista del artículo 12 inc. 5 que consagra la gratuidad, tal es el caso del derecho de bloqueo, por lo cual podría pensarse que para ejercerlo es necesario hacer valer una contraprestación. En este último escenario no nos estaríamos refiriendo a un derecho propiamente tal, sino más bien a una prestación de servicios y para ello habría que estarse a las normas de la ley del consumidor. No obstante lo anterior, la doctrina ha señalado que en caso de mediar un cobro, debiera ser racional y proporcional.

Con respecto al procedimiento general para hacer valer los derechos del titular contemplado en la LPDP art 16 inc. 2 letras a) y c), podemos encontrar una transgresión a la garantía constitucional de igualdad de las partes en el acceso a la justicia y como conclusión de esto una infracción a la garantía contenida en el debido proceso. Esto debido a que se señala en la letra a) que el titular de los datos debe presentar

inmediatamente la prueba cuando interpone una reclamación de lo contrario no podrá hacerlo en ninguna otra instancia, y por lo tanto su pretensión no puede en ningún caso verse acogida. Mientras que por otro lado la letra c) señala que el encargado del banco de datos puede solicitar que se realice otra audiencia para presentar la prueba en el caso de verse impedido de rendirla en la contestación del reclamo. Es evidente que esta situación es naturalmente más favorable para los encargados de los bancos de datos, es un error gravísimo por parte del legislador, sobre todo considerando la cercanía entre las disposiciones que contienen aquella patente desigualdad en un mismo artículo.

También encontramos otra falencia de la ley en el artículo 22 de la LPDP, el cual señala que "el Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos", básicamente este artículo es letra muerta debido a que esta institución no está facultada en ningún caso para exigirle a los organismos que realicen el tratamiento de los datos la adhesión obligatoria al registro de datos.

Podemos concluir tras el análisis de las criticas mencionadas anteriormente que existe una notoria sensación de malestar e inseguridad del titular de los datos, pues éste no puede sentirse amparado por el derecho de una forma efectiva y estructurada, puesto que si reuniéramos la gran cantidad de excepciones al consentimiento, la ausencia de la figura de la representación, el problema de la prueba en perjuicio del titular en el procedimiento general, entre otras, podemos señalar con toda certeza que es poco probable el éxito de la pretensión del titular ejercida con la finalidad de proteger sus derechos.

El Estado tiene el deber de brindar a través de las leyes una correcta protección a sus ciudadanos, y en el tema de protección de datos personales se encuentra en deuda, debemos aspirar a mejorar las falencias existentes y adecuarnos a los distintos tratados internacionales que regulan esta materia, así como, por ejemplo, el convenio de la OCDE, que establece normas básicas relativas a la protección de datos personales. El Estado no puede seguir más tiempo sin pronunciarse sobre ello, y se hace necesario que la legislación interna se adapte a los mínimos estándares que existen en los tratados internacionales relativos a la materia.

2.3.2 Críticas fuera de la ley: No existencia de un organismo fiscalizador, controlador, administrativo.

Una de las principales falencias que encontramos hoy en día en materia de protección de datos personales es la inexistencia de un órgano encargado de controlar, fiscalizar y asistir a los titulares frente a las vulneraciones que puedan sufrir a consecuencia del tratamiento de sus datos.

En la actual ley de protección de datos personales, específicamente en el artículo 22 se señala que "El Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos. Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende, todo lo cual será definido en un reglamento. El organismo público responsable del banco de datos proporcionará esos antecedentes al Servicio de Registro Civil e Identificación cuando se inicien las actividades del banco, y comunicará cualquier cambio de los elementos indicados en el inciso anterior dentro de los quince días desde que se produzca".

Si bien la disposición es positiva para el titular de los datos personales, es un poco idealista e ingenua, ya que en la praxis esta disposición no tiene gran aplicación. Esto ocurre en parte porque en la realidad no se lleva a cabo un registro de aquellos responsables que realizan tratamiento de datos, principalmente porque el Registro Civil no posee facultades de fiscalización en estos temas y no puede obligar ni compeler a ningún banco de datos a cumplir con esta normativa, lo que finalmente conlleva a que, al no sentirse obligados los bancos de datos sea muy improbable que cumplan con su obligación de informar respecto del tratamiento de datos que realizan para que el Registro Civil proceda a la elaboración del correspondiente registro.

Como vemos existe una carencia de un organismo fiscalizador de carácter preventivo/controlador o más bien un órgano cercano al titular que se dedique a orientarlo y asistirlo cuando crea que sus derechos han sido vulnerados, que vele por el correcto cumplimiento de la ley, la cual por cierto merece ser urgentemente reformada.

En caso de que existiera una modificación en la regulación concerniente a la protección de datos personales, una de las primeras interrogantes que deberíamos hacernos es si es necesario crear un organismo nuevo especializado en la materia, o bien, atribuirle esta tarea a algún organismo ya existente que sea capaz de flexibilizar sus funciones y se vea naturalmente apto para desempeñarse como tal.

En caso de decidir que es necesaria la creación de un órgano nuevo especializado en la materia debemos precisar si éste debiera ser un órgano de carácter público o privado. A modo de ejemplo, en España existe un órgano denominado Agencia Española de Protección de Datos (AEPD) (2014), ésta es la autoridad estatal de control independiente encargada de velar por el cumplimiento de la normativa sobre protección de datos. Garantiza y tutela el derecho fundamental a la protección de datos de carácter personal de los ciudadanos. 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 relaciona con el Gobierno a través del Ministerio de Justicia.

Como dijimos, en nuestro país solo existe la disposición fantasma de facultar al Registro Civil para llevar un registro de las entidades públicas que realicen tratamiento de datos. Hoy en día existe un proyecto de ley en tramitación que en síntesis viene a facultar al Servicio Nacional del Consumidor (SERNAC) para resolver estos temas, extendiendo sus facultades y sus competencias. Frente a esto, cabe cuestionarse si realmente es eficiente la idea de aumentarle la carga y extenderles la competencia a organismos que ya poseen funciones y objetivos claros.

Otra moción para poder solucionar este problema guardaría relación con la creación de una superintendencia, un organismo que pueda interponer multas en caso de incumplimiento por parte de los responsables de los bancos de datos, ya dichos órganos se encuentran facultados para hacerlo. O también otra alternativa sería designarle esta tarea a la Subsecretaría de Telecomunicaciones, otorgándole facultades de fiscalización y supervisión del manejo de la información en los distintos bancos de datos. Existe actualmente un proyecto de ley en trámite que acoge ampliamente la aplicación del derecho al olvido y le designa a este organismo la tarea de regularlo.

2.3.3 Críticas fuera de la ley: No existencia de un tribunal especial y competente en la materia

De nada sirve que exista un órgano que vele por el cumplimiento de la ley y asesore a los individuos, si no existe a su vez un tribunal especial que tenga jurisdicción para ejecutar el cumplimiento y generar resoluciones frente a distintas infracciones que se puedan producir, por lo que se hace necesaria la creación de esta entidad, la cual se especialice en lo que respecta a la protección de datos personales.

El derecho al olvido y la protección del titular en el tratamiento de sus datos personales es un tema altamente técnico y tecnológico. En este sentido, es necesario que los jueces encargados de tramitar estos

casos tengan conocimientos actualizados de la materia que les permita juzgar y resolver de la mejor manera.

Hoy en día son los tribunales civiles ordinarios quienes son los encargados de conocer y resolver los conflictos suscitados, siendo evidente que los jueces no tienen un conocimiento acabado y actualizado respecto al tema porque probablemente son inmigrantes de la tecnología, lo cual dificulta una correcta protección de los datos personales consagrados a los titulares.

Junto a lo anterior cabe mencionar que existe una alta tasa de congestión de casos dentro de estos tribunales, lo que complejiza aún más la situación, pues seguimos sobrecargando al sistema judicial.

Si bien la ley otorga la acción de Habeas Data para que los titulares hagan valer sus derechos frente a determinadas vulneraciones, el mecanismo más utilizado por los titulares no es este, sino que se trata del Recurso de Protección consagrado en nuestra constitución, esto se debe a que en teoría este les brindaría mayor protección pues puede fundamentarse de forma más amplia, cubriendo ciertas situaciones no previstas por la ley 19.628.

Como vemos, la creación de un tribunal especializado en la materia se hace necesario hacer un símil con lo que ocurrió en su momento en la problemática medioambiental en nuestra legislación.

El cuidado y preocupación por el medioambiente en el país ha ido creciendo aceleradamente en este último tiempo, lo que finalmente conllevó a que se decidiera legislar frente a este tema. Por ello se creó una ley, una superintendencia, un tribunal técnico y especializado y también un Ministerio de Medioambiente. Existe una voluntad del legislador para hacerse cargo de un problema y es por ello que se crea un conjunto completo e integral de órganos que pueden ocuparse del mismo tema de forma más profesional y especializada.

El Ministerio y la Superintendencia de Medioambiente no tienen muchos años desde que han comenzado a funcionar, sin embargo, desde su primera fase, el Tribunal Medioambiental ha ayudado en la descongestión de los casos de recurso de protección referentes a la materia medioambiental de los que se encargaba la Corte Suprema.

Hoy en día existe esta misma necesidad en relación a la protección de datos, por lo que la existencia de un tribunal que conozca y resuelva los casos suscitados en esta materia, ayudaría a que los titulares de los datos personales confíen en el sistema judicial, y, además, apoyaría en la resolución de la gran cantidad de recursos de protección sometidos a conocimiento de las Cortes de nuestro país.

2.4 Proyectos y reformas hechas en materia de protección de datos personales.

Como mencionamos con anterioridad, la ley 19.628 sobre protección a la vida privada y los datos personales, fue promulgada el 18 de agosto del año 1999. Han transcurrido más de 20 años aproximadamente desde su promulgación. Evidentemente es una ley que hoy en día se encuentra un tanto obsoleta y anticuada debido a que abarca situaciones y circunstancias que se daban en la época de su creación, cuando recién comenzaba el auge de internet como un medio masivo de comunicación, encontrándose en una etapa inicial que no se puede comparar con la importancia y los avances tecnológicos que existen en la actualidad, ya que internet se ha convertido en un elemento esencial en el desenvolvimiento de las personas dentro del entorno social y en su calidad de vida. La tecnología se ha vuelto sumamente importante para diversas áreas de desarrollo de los chilenos, por ejemplo, en áreas laborales, de emprendimiento, como fuente de información, e incluso como medio de esparcimiento y entretención.

Es por esto que el tratamiento y tráfico actual de datos, sean estos personales o no, se han masificado enormemente debido a la aparición de las nuevas tecnologías y del desarrollo avanzado que ha experimentado internet. Este último se ve reflejado en las diversas estadísticas realizadas por la Subsecretaria de las Telecomunicaciones (SUBTEL). Una de ellas se realizó a finales del año 2013, la cual viene a evidenciar que la penetración de internet, fijo y móvil pasa desde 13,7 accesos por cada 100 habitantes en 2009 a 49,0 accesos cada 100 habitantes. Señalando asimismo que más del 68% de los chilenos son usuarios de internet, y que Chile se ubica en el lugar 23 del mundo dentro del ranking mayor cantidad de personas denominadas como nativos digitales, existiendo un 92,4% de jóvenes conectados entre 15 y 25 años.

Los nativos digitales corresponden a aquellas personas que nacen en un "mundo tecnológico", es decir, que desde temprana edad presentan conexiones con la tecnología y el internet, por lo cual poseen un grado de destreza mayor en el uso y manejo de las mismas, siendo estos uno de los entornos en los que mayormente se desenvuelven. Y se sienten protegidos en los contextos virtuales, lo que los lleva a compartir sus vidas allí, algunas veces sin pensar demasiado sobre el hecho de que sus datos, reflexiones, información y contenidos quedan en las redes y podrían ser conocidos casi por cualquier persona, tanto ahora como en muchos años más.

En la vereda opuesta nos encontramos con aquellas personas denominadas 'inmigrantes de las tecnologías', entendiéndose por estas, aquellas que nacieron y crecieron en un entorno en el que la tecnología y el internet no se encontraban masificados ni desarrollados, conectándose de adultos a este

“mundo tecnológico”, por lo que a diferencia de los nativos, son personas que se mantienen más cautos respecto a la información de datos personales que comparten.

Más allá de las diferencias generacionales y los resquemores, con más o menos precaución, en la actualidad tanto nativos como inmigrantes comparten grandes volúmenes de información personal en plataformas de redes sociales, ya sea para comunicarse, entretenerse o, simplemente, para compartir contenidos. (Baytelman, 2011)

En estadísticas más actuales realizadas por la SUBTEL respecto del crecimiento y aumento de internet en Chile la penetración de internet fijo y móvil (3G+4G) pasó de 52,1 accesos por cada 100 habitantes en marzo 2014 a 64,2 accesos cada 100 habitantes en el mismo mes del año 2015.

Queda evidenciado entonces que existe un aumento progresivo a gran escala respecto al desarrollo de las tecnologías y el acceso a internet por parte de los ciudadanos chilenos, lo que consecuencialmente produce una masificación en el tratamiento, el traspaso y el compartimiento de datos personales, hecho que finalmente podría terminar conculcando los derechos de las personas relativos a la protección de dichos datos si es que no se realizan las modificaciones correspondientes y atingentes a los avances tecnológicos que se dan en la actualidad, resultando apremiante realizar una reforma integral a la ley 19.628.

Si bien se han realizado un número importante de proyectos de reformas constitucionales y legales respecto de la protección de los datos personales, la vida privada y todas las materias atingentes al caso, muchos de ellos no han prosperado en su tramitación y se encuentran “durmiendo” en nuestro órgano legislador, o bien, han sido directamente desechados.

Sin embargo, hoy en día podemos decir que existen algunos avances al respecto, siendo unos de los más importantes el boletín N° 9384-07 el cual tenía por objeto modificar nuestra carta fundamental, siendo ingresado al congreso el día miércoles 11 de junio del año 2014. Este proyecto de ley tenía por finalidad consagrar un derecho fundamental que reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos, es decir, que las personas puedan tener control respecto de sus datos personales y su correspondiente protección.

Como mencionamos en capítulos anteriores, en nuestro país si existe la consagración del Habeas Data, esto es, el derecho absoluto de toda persona a acceder ya sea administrativa o judicialmente, a la información que se tenga de ella, así como también pedir su correspondiente modificación, eliminación o bloqueo. No obstante, dicho derecho solo es de rango legal, pues se encuentra establecido en el artículo dieciséis de la Ley 19.628, por lo que esta nueva reforma viene a elevar la consagración del Habeas Data

a rango constitucional, estableciendo un derecho independiente y autónomo de aquellos derechos que, si bien se relacionan entre sí, como lo son el derecho de privacidad, la honra, entre otros, más no cubren las necesidades específicas en esta materia. Fue así como finalmente, y luego de varios años de espera, tuvimos un gran avance en materia de protección de datos personales, puesto que el día martes 15 de mayo del año 2018 fue aprobado dicho proyecto de ley, procediéndose a la modificación del artículo 19 N°4 de nuestra Constitución Política mediante la promulgación de la ley 21.096, señalando ahora que la constitución asegura "El respeto y protección a la vida privada y a la honra de la persona y su familia, **y, asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley**". Esta última parte finalmente conlleva a consagrar al derecho a la autodeterminación informativa, y, tal como señala el Boletín N° 9.384-07 (2014) se trata "pues, de un derecho constitucional autónomo, que si bien reconoce su origen en el derecho a la intimidad, está dotado de un contenido diferente", y consiste en el derecho de las personas a controlar sus datos personales, incluso si estos no se refieren a su intimidad, existiendo una especie de control previo positivo, al poder las personas determinar quiénes pueden acceder a sus datos e información personal.

La antes mencionada reforma constitucional es uno de los escasos cambios que se han materializado en los últimos tiempos en nuestra legislación respecto a la protección de datos personales, y, como apreciamos, solo viene a darle un rango constitucional, mas no viene a realizar una modificación integral y actual en la materia, por lo que nuestro país se encuentra al debe con los ciudadanos. Frente a esta situación y con la intención de regular esta situación es que se refunden dos proyectos de ley, a saber, los boletines 11.144-07 y 11.092. Esta iniciativa se origina en Mensaje que ingresó al Senado el 15 de marzo de 2017, y viene a modificar sustancialmente la Ley de Protección de Datos N° 19.628. Lo anterior es con la finalidad de actualizar la legislación en materia de protección de datos a las condiciones y estándares internacionales que existen en la actualidad.

Este nuevo proyecto refundido fue aprobado en general por el Senado el martes 3 de abril de 2018, por 42 votos a favor y una abstención. Posteriormente en marzo de 2020, luego de la discusión particular al que fue sometido dicho proyecto, es aprobado por unanimidad en la Comisión de Constitución del Senado, pasando así a revisión por parte de la Comisión de Hacienda, por lo que ahora para que se transforme en ley falta su discusión en la Cámara de Diputados, es decir, debe pasar por el segundo tramite constitucional.

A continuación, pasaremos a analizar dicho proyecto señalando las principales reformas y novedades que pretende introducir relacionadas a la protección de datos.

a) A diferencia de la actual legislación, este nuevo proyecto de ley viene a establecer expresamente ciertos principios que regularán y regirán el uso de los datos personales, su tratamiento y su conservación. Son principalmente 8 los principios rectores a saber: Principio de Licitud; Principio de Finalidad; Principio de Proporcionalidad, Principio de Responsabilidad; Principio de Transparencia e Información; Principio de Confidencialidad y; Principio de Calidad.

   Evidentemente era necesario que una regulación estipulara de forma clara y expresa los principios rectores que deben informar la protección de los datos y su correspondiente tratamiento, ya que a falta de alguna norma expresa en determinados asuntos, los principios juegan un rol primordial para la resolución de un conflicto.

b) La actual legislación establece el consentimiento del titular como regla general para realizar el tratamiento de sus datos, lo cual se mantiene en esta reforma, sin embargo, establece y regula los requisitos que debe cumplir este para ser válido y producir efectos, a diferencia de lo que se señala en el actual artículo cuarto de la ley 19.628, que solo exige que se preste por escrito, requisito que deja de existir en el nuevo proyecto de reforma. Este último viene a definir el consentimiento como aquella manifestación de voluntad libre, específica, inequívoca e informada, supliendo entonces una de las falencias que mencionamos anteriormente de la actual legislación. Se mantiene la posibilidad de revocar dicho consentimiento prestado, la que solo producirá efectos hacia el futuro y no así en tratamiento de datos realizado en tiempo intermedio.

   Otro hito importante respecto al consentimiento, es que esta nueva reforma añade una presunción de que, a pesar de la existencia de consentimiento por parte del titular de los datos personales, este no será fuente de licitud para tratamiento cuando exista un desequilibrio evidente entre la posición del titular y el responsable, presentándose este cuando el tratamiento de dichos datos se basa en un consentimiento otorgado para la ejecución de un contrato o la prestación de un servicio que no requieren del tratamiento de datos personales para su ejecución o cumplimiento. Sin embargo, existe una excepción a esta presunción y se trata de aquellos casos en que se ofrezcan bienes, servicios o beneficios, siempre y cuando, quien los ofrezca requiera como única contraprestación el consentimiento para tratar datos.

c) En relación con el punto anterior, otra de las novedades del proyecto dice relación con la incorporación de nuevas fuentes de licitud para realizar el tratamiento de datos personales, fuera de los ya mencionados por la actual legislación, que son el consentimiento del titular y la autorización legal. Señalando que será licito el tratamiento incluso sin consentimiento de los titulares cuando los datos sean: recolectados de una fuente de acceso público y su tratamiento

esté relacionado con los fines para los cuales fueron entregados; o cuando el dato es relativo a obligaciones de carácter económico, financiero, bancario o comercial; o si el tratamiento es necesario para la ejecución o cumplimiento de una obligación legal; o si el tratamiento es necesario para la celebración o ejecución de un contrato entre el titular y el responsable; o si el tratamiento es necesario para la satisfacción de intereses legítimos del responsable o de un tercero, siempre que no se afecten los derechos y libertades del titular; o si es necesario para la defensa de un derecho en juicio. (Carey & Silva, 2018).

d) Otra novedad de esta reforma dice relación con los datos de carácter sensibles, según la actual legislación su tratamiento se encuentra prohibido, salvo que una ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares, sin realizar distinción alguna respecto al tipo de dato sensible al que corresponda. En cambio, en el nuevo proyecto se señala que estos datos solo podrán tratarse con el consentimiento expreso del titular, el cual puede ser otorgado a través de una declaración escrita, verbal o por un medio tecnológico equivalente. Y señala la existencia de datos sensibles que poseen regulación especial, estos son: datos sensibles relativos a la salud; datos relativos al perfil biológico humano y; datos personales biométricos.

e) Junto a lo anterior, en este nuevo proyecto de ley se establecen ciertos datos correspondientes a categorías especiales, o que establecen normas diferenciadas en cuanto a su tratamiento. Por ejemplo, tenemos el caso de los datos personales correspondientes a niños y adolescentes, quienes en la actual legislación no tienen un tratamiento especial a pesar de su condición, sin embargo, con este proyecto se establece que, por regla general, los datos que correspondan a menores de 14 años solo pueden tratarse previa autorización de sus padres o representantes y atender a su interés superior, respetando su autonomía progresiva. Mientras que respecto de aquellos menores de 18 años, pero mayores de 14 les serán aplicables las reglas correspondientes al tratamiento que aplica para los adultos, exceptuándose a esta regla, solamente aquellos datos de carácter sensibles, los que deberán ser objeto de autorización de sus padres o representantes.

   Las otras categorías especiales de datos corresponden a aquellos datos de geolocalización, así como también a aquellos datos tratados con fines históricos, estadísticos, científicos y de estudios o investigaciones con fines de interés público.

f) Este nuevo proyecto a su vez, viene a regular de forma clara y específica los derechos que se le otorgan a los titulares de los datos personales, siendo estos: (i) Derecho de Acceso, que consiste en solicitar y obtener confirmación acerca de si sus datos personales están siendo tratados; (ii)

Derecho de Rectificación, este derecho aplica cuando los datos son inexactos, desactualizados o incompletos, y se faculta al titular a solicitar la modificación de los mismos para que vuelva a ser lícito su tratamiento; (iii) Derecho de Cancelación, este derecho consiste en la facultad que tiene el titular de solicitar la destrucción o supresión de sus datos personales, señalando la misma ley un catálogo de situaciones en las que especialmente se puede ejercer dicho derecho, como por ejemplo cuando ya no se cumpla la finalidad por la cual se inició su tratamiento o el titular revoque su consentimiento, entre otras. Sin embargo este derecho no es absoluto ya que se mencionan ciertos escenarios en los cuales no procede su ejercicio; (iv) Derecho de Oposición, corresponde al derecho de solicitar que no se lleve a cabo un tratamiento determinado de datos siempre y cuando se den determinadas circunstancias, como por ejemplo cuando se afectan los derechos y libertades fundamentales de los titulares, o si el tratamiento se realiza exclusivamente con fines de mercadotecnia o marketing directo de bienes, productos o servicios, entre otras; y (v) Derecho de Portabilidad, este último consiste en la facultad de obtener una copia de los datos personales entregados al responsable del tratamiento de manera estructurada, en un formato genérico y de uso común, que permita ser operado por distintos sistemas con la finalidad de comunicarlos a otro responsable para que realice su correspondiente tratamiento siempre y cuando sea realizado en forma automatizada y esté basado en el consentimiento del titular.

Cabe destacar que estos derechos son de carácter personal, intransferibles e irrenunciables, pero pueden transmitirse a los herederos del titular, excepto cuando la persona fallecida lo hubiese prohibido expresamente o la ley así lo estipule.

g) En la actual legislación, para hacer valer los derechos asegurados a los titulares de datos, contamos con la acción de Habeas Data, la cual se puede ejercer a través de tres procedimientos, a saber: procedimiento general que opera cuando, o no se pronuncia, o se deniega la reclamación por parte del responsable del tratamiento de datos aludiendo a causales que no corresponden a la seguridad de la Nación o al interés nacional; procedimiento especial, es el que opera en caso de que las causales en las que se fundamenta la denegación de la solicitud del titular de los datos sea por seguridad de la Nación o en virtud del interés nacional y; procedimiento sumario, aquel que tiene el carácter de ser residual ya que para todas las demás acciones no contempladas en los procedimientos anteriores deberá conocerse mediante las reglas del juicio sumario. Como vemos, en la ley actual se contemplan tres tipos de procedimientos, mientras que la nueva reforma viene a cambiar las reglas y procedimientos estipulados, señalando la existencia de los siguientes: (i) Procedimiento administrativo de tutela de derechos: se ejerce por el titular ante el Consejo para la Transparencia y Protección de Datos Personales, y procede cuando el

responsable haya denegado al titular una solicitud para ejercer cualquiera de los derechos que le reconoce la ley o bien cuando no haya dado respuesta a dicha solicitud dentro del plazo correspondiente. (ii) Procedimiento administrativo por infracción de ley: Es instruido por el Consejo para la Transparencia y la Protección de Datos Personales como resultado de un proceso de fiscalización o a consecuencia de una reclamación presentada por un titular, para la determinación de infracciones por incumplimiento de los principios, derechos y obligaciones establecidas en la ley. (iii) Procedimiento de reclamación judicial: Las personas naturales o jurídicas que estimen que un acto administrativo que paraliza el procedimiento, o una resolución final o de término emanado del Consejo, sea ilegal y les cause perjuicio podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones competente, en 15 días desde la notificación de la resolución impugnada. (Carey & Silva, 2018).

h) Sin lugar a duda una de las mayores novedades que incorpora este nuevo proyecto es la designación del Consejo para la Transparencia como la autoridad de control de la protección de datos personales, estando encargado de velar por el cumplimiento de la normativa relativa al tratamiento de datos personales y su protección, como de todos los derechos consagrados en esta ley", Este organismo contará con diversas funciones y facultades, las cuales se encontraran reguladas en la ley, destacando por ejemplo que podrá proponer al Presidente y al Congreso Nacional normas legales y reglamentarias, deberá resolver las solicitudes y reclamaciones realizadas por los titulares de datos, le corresponderá aplicar e interpretar administrativamente las disposiciones legales y reglamentarias cuyo cumplimiento le corresponda vigilar, deberá administrar el Registro Nacional de Cumplimiento y Sanciones, entre otras.

i) Esta nueva reforma viene también a regular un tema importante que hasta el día de hoy nadie se había hecho cargo, nos referimos a la transferencia internacional de datos. Como hemos mencionado la tecnología ha avanzado a pasos agigantados en los últimos años, lo que ha conllevado a que nuestros datos personales puedan ser compartidos incluso traspasando las fronteras. Es sumamente necesario regular lo sucedido con este traspaso internacional de datos, y eso pretende el nuevo proyecto, el cual viene a establecer en qué casos ella se considerará lícita. Y será la Agencia el organismo encargado de fiscalizar las operaciones de transferencia internacional, pudiendo formular recomendaciones, adoptar medidas conservativas y en casos calificados, suspender temporalmente el envío de los datos. (Carey & Silva, 2018).

Como vemos esta nueva iniciativa de reformar la regulación actual en materia de protección de datos personales viene a hacerse cargo de las falencias y carencias de la actual legislación, reformando íntegramente la ley 19.628, regulando aspectos tan importantes como los que mencionamos y otros más.

2.5 Visión de la jurisprudencia ante el derecho al olvido.

Como vemos, en Chile existe la ley 19.628 que regula la protección de los datos personales, estableciendo ciertos derechos en caso de que los titulares de los mismos se vean vulnerados por los responsables de su tratamiento. Dichos derechos se ejercen mediante la acción de Habeas Data consagrada en su artículo 16, la cual debe ejercerse mediante un procedimiento que presenta reglas especiales señaladas en el mismo artículo en comento. Sin embargo, cabe señalar que al proceder esta acción especial en determinadas circunstancias y bajo ciertos presupuestos, los titulares de los datos personales optan por interponer el Recurso de Protección estipulado en nuestra Constitución Política, pues da la posibilidad de argumentar ampliamente y así abarcar casos que quizás no serían amparados bajo la ley 19.628.

A continuación pasaremos a exponer algunos casos jurisprudenciales en los cuales se aborda el Derecho al Olvido por nuestros tribunales nacionales, existiendo casos en que este ha sido acogido y reconocido, mientras que por otro lado nos encontramos con una postura distinta denegando las pretensiones que aspiraban a obtener la eliminación de datos personales.

1. Sentencia Rol 228-2012

Un ciudadano interpone recurso de protección ante la Corte de Apelaciones de Valparaíso en contra de todos aquellos responsables que resulten ser administradores del sitio de búsqueda de páginas de internet denominado “google.cl”, y del administrador de correos electrónicos denominado “gmail.cl”, junto con otros sitios de internet, señalando que en ellos aparecen difundidas afirmaciones de carácter totalmente injuriosas como asimismo calumniosas en contra de su personas, su cónyuge, hijos y familia, lo cual afecta el derecho de honra y respeto a la vida privada. Ante esto solicita que la Corte ordene la eliminación de toda información injuriosa en contra suya y de su grupo familiar.

Ante estos hechos la Corte de Apelaciones ordena en su fallo la “eliminación en las respectivas páginas web mencionadas a fs. 12, de las informaciones injuriosas que en ellas se consignan, lo que se hace extensivo a las páginas web de la cuenta de correo correspondiente y blogspot”, debido a que efectivamente estas publicaciones injuriosas vulneraban los derechos amparados por nuestra Constitución en el artículo 19 N°4. Junto a lo anterior, ordena también “que el buscador “google.cl” establezca computacionalmente los filtros necesarios para evitar publicaciones que presenten inequívocamente publicaciones de carácter injurioso, o de cualquier tipo y bajo cualquier circunstancia, siempre que en esa publicación se incurra en una afectación constitucional como la mencionada, todo ello bajo los apercibimientos que establece el citado del Auto Acordado sobre la materia”. Esto último es un importante precedente en cuanto a la responsabilidad que se les atribuye a los motores de búsqueda

en el tratamiento de los datos personales, lo que se asimila un poco al caso de Google Inc. contra la Agencia Española de Protección de Datos y Costeja. Existe en la sentencia claramente un acogimiento del incipiente derecho al olvido por parte de la Corte, y cabe destacar que no es solo en contra de los motores de búsqueda que establece la eliminación de la información, sino que además obliga a las páginas web y sitios de internet que publicaron dicha información injuriosa a borrar dicho contenido, por lo que se aplica a cabalidad el concepto de Derecho al Olvido.

2. Sentencia Rol 22243-2015

Este caso corresponde a un ciudadano que interpone Recurso de protección ante la Corte Suprema, solicitando la eliminación de una noticia existente en una página web de un conocido diario nacional, la cual fue publicada el 17 de agosto de 2004, señalando esta que el recurrente era un oficial de Carabineros de Chile procesado como autor del delito de abuso sexual. Fundamenta su petición en que este hecho vulnera sus derechos de integridad física y psíquica, así como también la protección a la vida privada de él y su familia, y, que ambos derechos están amparados por el artículo 19 N° 4 de la Constitución Política.

Por su parte el recurrido señalaba que no procedería a borrar dicha información invocando su derecho de libertad de informar, mencionando además que el afectado tiene otros procedimientos especiales, y que debería proceder a través del ejercicio de la acción de aclaración o rectificación, y no mediante el presente recurso de protección.

La Corte Suprema viene a sentar un precedente en esta materia, ya que a pesar de indicar que "no existe, por ahora, una solución legislativa expresa sobre este tema", realiza un razonamiento jurídico tal, que logra fundamentar el acogimiento del Derecho al Olvido en nuestro país. En primer lugar, busca fundamento jurídico en nuestra propia Constitución, específicamente en el artículo 19 N° 4 y 5, pues señala que el derecho al olvido en parte busca proteger derechos tales como el honor, la privacidad y la dignidad de las personas. Además de ello, viene a señalar que este derecho se desarrolló por primera vez en materia penal, señalando que "si la propia ley penal –la más gravosa desde el punto de vista de la afectación de los derechos individuales– es la que señala un tiempo específico de duración de la pena, y permite además eliminarla de todos los registros públicos una vez cumplida esta, con mayor razón los medios de comunicación social deben actuar en coherencia con la intención de proporcionar al penado la posibilidad de desarrollar una vida acorde con el respeto a sus garantías constitucionales una vez transcurrido el tiempo de condena".

Junto con los fundamentos anteriores, la Corte Suprema también se apoya en normativas internacionales y derecho comparado, citando entre ellas a la Declaración Universal de los Derechos Humanos de las

Naciones Unidas, la Convención Americana de Derechos Humanos, incluso se apoya en el que en ese entonces era solamente un proyecto en estado de tramitación y no una normativa vigente en la Unión Europea. Nos referimos al Reglamento General de Protección de Datos Personales", que recién entró en vigencia en el año 2018.

Este fallo también es importante en nuestra jurisprudencia ya que la Corte Suprema viene a dar una definición de lo que se entiende por derecho al olvido, señalando que "se refiere sustancialmente a que una persona pueda aspirar a la eliminación de una información desfavorable sobre sí misma que le provoque perjuicios actuales y que se contenga en los sistemas informáticos disponibles, y ello por una razón plausible". Por primera vez nos aproximamos a una definición de lo que se entiende por Derecho al Olvido de nuestros tribunales, sentando un precedente en esta materia para futuras decisiones y fallos emitidos por la jurisdicción.

3. Sentencia Rol 36739-2017

Un ginecólogo interpone recurso de protección ante la Corte de Apelaciones de Santiago en contra de la Fundación Centro de Investigación Periodística (Ciper-Chile) por una publicación realizada hace 4 años en su página web, en la cual se realizó una investigación periodística que denunciaba a dicho ginecólogo por realizar prácticas inadecuadas consistentes principalmente en utilización de recetas falsas para conseguir Mysotrol en el extranjero y su posterior administración a una paciente con la finalidad de acelerar su parto. Ante esto el ginecólogo fundamenta la interposición del recurso en que su derecho a la protección de la vida privada y a su honra y la de su familia se habían visto vulnerados, ya que una página de Facebook había compartido nuevamente dicha publicación de Ciper-Chile, lo que habría generado una serie de comentarios en contra de su persona ocasionándole perjuicios. Frente a la solicitud de eliminar el contenido de la noticia en comento, la Corte de Apelaciones de Santiago decidió rechazar la petición del recurrente, decisión que fue ratificada por la Corte Suprema, fundamentando que "no se puede atribuir la comisión de acto ilegal alguno, toda vez que esta se limitó a publicar antecedentes de una investigación periodística respecto de la cual los hechos que la motivaron resultaron probados, al punto que significaron la aplicación de una sanción al recurrente por parte del Colegio Médico, debido al otorgamiento de recetas médicas falsas del medicamente denominado Mysotrol, situación que justifica plenamente la necesidad de hacer pública la información, debido a su relevancia y connotación". Por lo tanto, esta sentencia viene a señalar y establecer que siempre y cuando una noticia cumpla con requisitos o estándares de relevancia y veracidad debe prevalecer antes que el interés individual de la persona que ve afectados sus derechos de privacidad y honra del afectado y su familia, sentando un precedente

negativo para una posible aplicación del derecho al olvido en nuestra jurisprudencia. Cabe señalar que esta decisión no rechaza del todo una posible aplicación del Derecho al Olvido en general, sino más bien señala que siempre y cuando la noticia tenga ciertas características este no tendría lugar, por lo que podemos concluir que en todos los otros casos en que una publicación dañe y afecte los derechos de privacidad y honra de una persona, esta debería poder ser eliminada.

Cabe señalar también que en este fallo de la Corte Suprema no se obligó a eliminar la publicación realizada por Ciper-Chile por lo que mencionamos anteriormente, pero también porque es una página de Facebook quien viene a revivir esta noticia cuatro años después y no el recurrido, quien no tiene injerencia ni vinculación alguna con quienes realizaron la publicación que conllevó a los comentarios negativos que le ocasionaban perjuicios al recurrente, razón por la cual señala la sentencia que "quedan a salvo para el recurrente el ejercicio de las acciones legales que corresponden y que expresamente ha contemplado el ordenamiento jurídico en estos casos" en contra de los que resulten responsables de dicha publicación en la página de Facebook.

4. Sentencia Rol 11746-2017

En este caso un ciudadano interpone recurso de protección ante la Corte de Apelaciones de Santiago en contra de Google Inc. y otras páginas web de diversos diarios nacionales, los cuales en el año 2008 publicaron noticias relativas a la comisión de los delitos de abuso sexual y robo por parte del recurrente, el cual posteriormente en el año 2009 fue condenado como autor de los mismos, cumpliendo su condena en el año 2012. Sus antecedentes fueron borrados en octubre de 2014 en virtud de lo establecido en el Decreto Ley N°409. En dicho recurso fundamenta el recurrente que la mantención de las publicaciones en las páginas webs y la correspondiente indexación de estas en el motor de búsqueda de Google Inc., le ocasionan perjuicios en su derecho al honor, a la protección de la integridad síquica y a la libertad de trabajo, amparados en el artículo 19 Ns. 4°, 1° y 16° de la Constitución Política, por lo que exige la aplicación del Derecho al Olvido, solicitando la eliminación de los enlaces en los resultados de búsqueda, así como también la eliminación misma de las páginas web en las que se publicaron los hechos delictivos. La respuesta de la Corte de Apelaciones ante la petición del recurrente fue negativa, por lo que decidió apelar ante la Corte Suprema, quien ratificó el fallo de primera instancia.

La Corte Suprema señala en primer lugar que "el denominado derecho al olvido que invoca el recurrente no está establecido en nuestra legislación, por lo que la decisión de otorgar la cautela jurisdiccional que se invoca en autos debe ser analizada bajo el prisma de los derechos que se pueden ver afectados, el de la libertad de información y el derecho a la honra o en su caso, como sostienen algunos autores, el derecho a la vida privada". Como vemos realiza la prevención de que no existe en nuestra actual legislación el

establecimiento de un derecho al olvido propiamente tal, sino que se busca la aplicación de este a través del recurso de protección fundamentado en el amparo de otros derechos que se ven subsumidos por el derecho al olvido, los cuales son principalmente el derecho a la honra, a la vida privada y a la integridad psíquica, entre otros. Se señala que el concepto de derecho al olvido "está siendo construido por la doctrina y la jurisprudencia, en virtud del principio de la inexcusabilidad que informa la actuación de los tribunales".

Sin embargo, en este caso la Corte Suprema al realizar una ponderación del conflicto de los derechos en juego, señala que "es claro que existe un interés público en que la información sea conocida, razón por la cual, la libertad de información prevalece sobre el derecho a la honra y a la privacidad que invoca el recurrente", entonces se previene que "son las particularidades de cada caso las que inciden en la formación de la convicción que lleva a resolver en un determinado sentido", ya que al tratarse en este caso de la comisión del delito de abuso sexual hace que la noticia sea de relevancia y de interés público para la sociedad en general, debiendo mantenerse las publicaciones correspondientes, ya que según Nogueira (2004) "la relevancia pública de la información es la única causa de legitimación para afectar el derecho a la privacidad".

Cabe mencionar que este fallo de la Corte Suprema no fue acordado por unanimidad de sus miembros, ya que hubo un voto disidente del Ministro Aránguiz, quien se mostró dispuesto a acoger el recurso de protección en favor del recurrente, fundamentando su postura principalmente en que "el referido "interés público" es en sí un criterio demasiado amplio" y que "un factor objetivo al respecto, es el transcurso del tiempo, porque salvo en los delitos de lesa humanidad, imprescriptibles e inamnistiables, aún los delitos más graves merecen el perdón de la sociedad que, otra cosa no es el "derecho al olvidar"" y que este criterio objetivo del transcurso del tiempo "tiene una fuerte raigambre en el espíritu general de nuestra legislación, con la institución denominada "prescripción"", y que por lo tanto si el tiempo máximo en que prescriben incluso delitos más graves, como por ejemplo el homicidio, son 10 años, este parecería un "transcurso de tiempo suficiente para que, contado desde la fecha del cumplimiento de una condena, pueda entenderse terminado el "interés público" para mantener la información del hecho "en el aire" y a partir de entonces se la pueda aludir sin los datos personales del individuo actor".

Como se puede apreciar este fallo tiene especial relevancia, ya que, a pesar de haberse denegado la Corte Suprema a aceptar el acogimiento del derecho al olvido, se señala que esta decisión se adopta principalmente atendiendo a las circunstancias del caso en particular, dejando cabida para una futura aplicación en otros casos que se susciten más adelante. Además de esto, el voto disidente de uno de los ministros y su correspondiente fundamentación deja ver que no existe una postura única y tajante

respecto al derecho al olvido y su aplicación en nuestro país, por lo que es un tema que sigue desarrollándose casuísticamente.

Conclusiones

Como pudimos apreciar a lo largo del presente trabajo el derecho al olvido es un derecho insipiente que poco a poco ha ido tomando fuerza en la última década, pasando de ser un asunto totalmente desconocido y poco regulado, a uno de los temas que se encuentra en boga en los últimos años. Claramente uno de los hitos que evidenció la falta de legislación respecto a la protección de datos personales y más específicamente del derecho al olvido, fue el caso que inició en el año 2010 el ciudadano español Mario Costejas contra uno de los motores de búsqueda de internet más importantes del mundo, nos referimos a Google. Dicho caso fue iniciado en España, y posteriormente fue tomando connotación a nivel continental, pasando a ser revisado por el Tribunal de Justicia de la Unión Europea, lo que posteriormente conllevó a que fuera conocido mundialmente, pues la resolución que se le dio al caso vino a sentar un gran precedente, dando por primera vez cabida al derecho al olvido y asegurando en cierta medida la protección de los datos personales de Costejas, al ordenar al motor de búsqueda la eliminación de sus resultados del enlace de la correspondiente página web que contenía la información cuya eliminación había solicitado por causarle perjuicios.

Este y otros casos, como el de Google contra Francia, dejan demostrado que no existen casos en que se haya otorgado completamente la eliminación pertinente y completa de la publicación que contiene la información privada de un sujeto, ya que dicha obligación solo respecta a los motores de búsqueda y a niveles nacionales, es decir, solo desaparece de “google.es” y “google.fr” respectivamente, ya que no existe una obligación de eliminar los enlaces de las páginas web en todos sus dominios a nivel mundial. En base a estos antecedentes podríamos decir que una de las principales críticas que podemos apreciar y reflejar en el presente trabajo, es el hecho relativo a la sustantividad del derecho al olvido. Cabe preguntarse si posee cierto grado de autonomía en su ejercicio.

Frente a estos cuestionamientos podríamos señalar que no se trata de un derecho independiente y absoluto, ya que al momento de ejercer el derecho al olvido nos encontramos con limitaciones y barreras que hacen casi imposible una aplicación per se, como es el caso de la pugna existente con la libertad de expresión, la no existencia de censura previa, el libre acceso a la información, entre otros derechos, que hacen sumamente necesaria una flexibilización en su aplicación.

A lo anterior se suma otra problemática relativa al costo económico que acarrea su implementación, esto debido a que muchas veces el costo de eliminación de la información publicada en una página web es más grande que el perjuicio sufrido por la víctima.

Como podemos apreciar son diversas las críticas que recibe el incipiente Derecho al Olvido, pero creemos que frente a ellas existen a su vez distintas maneras de mejorar dicho derecho, soluciones que asegurarían una correcta y sistemática aplicación del Derecho al Olvido, evitando los conflictos suscitados entre derechos como la libertad de expresión, los DDHH, la honra, la dignidad, la privacidad, entre otros.

Dentro de las posibles medidas a implementar en el tratamiento de datos personales en internet como forma de solucionar las problemáticas existentes en el derecho al olvido, nos encontramos con la idea de establecer una fecha de caducidad, lo que permitiría que la información que se suba a la red y que contenga datos de carácter personal sea válida por cierto periodo o lapsus de tiempo, y que una vez llegada la fecha límite establecida desaparezca automáticamente de la web, esto se condeciría con el principio de finalidad, pues dicha información ya no cumple con los fines que se tuvieron en consideración al momento de publicarla. Con ello la información que contiene datos personales caducaría y se eliminaría automáticamente. Sin embargo, las personas que descargan y guardan el contenido de las páginas webs, es decir del contexto original, fácilmente pueden compartir nuevamente la información, a pesar de que la original o inicial haya sido eliminada. Frente a esta problemática la solución sería que esta fecha de caducidad se transmitiera a todas las copias que se realicen de dicha información, pasando a convertirse en una característica más del archivo o documento original, tal como el nombre, su extensión, etc., y con esto cualquier copia de la información original se eliminará en las mismas condiciones que ella una vez cumplido el vencimiento del plazo.

Otra de las soluciones plausibles es la contextualización, la cual consiste en que cada vez que exista información que no sea actual o verídica respecto de una persona, esta podría en el mismo artículo o página web donde se contienen sus datos, realizar una aclaración o rectificación de la información, de manera que esta quede glosada a la anterior y llegue al público de la misma forma que la información original. Para que este sistema de solución pueda llevarse a cabo la persona debe estar en conocimiento de todas las publicaciones que hagan referencias a sus datos personales, frente a esto cabe preguntarnos ¿Cómo una persona puede enterarse de las publicaciones que circulan en la web? ¿Qué herramientas podrían utilizarse para notificar a la persona que se está dando información respecto de su persona? La respuesta a estas interrogantes podría ser la etiquetación forzosa de la persona en cualquier artículo que contenga sus datos personales. No obstante, para que esto funcione de manera efectiva, debería crearse una ley que obligue a los controladores de la información a etiquetar obligatoriamente a la persona cuando sus publicaciones hablen o hagan referencia de sus datos personales.

Sin embargo, algunos señalan que esta herramienta no es suficiente en todos los casos, por lo que creemos que por sí sola no funciona correctamente en todos los casos, razón por la cual creemos que sería

conveniente que tanto la contextualización como la fecha de caducidad, se implementaran conjuntamente, lo cual ayudaría a mejorar la aplicación del Derecho al Olvido, convirtiéndolo en un derecho de aplicación sistemática, que estaría regulado concretamente por las regulaciones internas de cada país, o mejor aún por regulaciones internacionales entre los diversos países, consiguiendo con ello la aplicación y efectividad global del Derecho al Olvido respecto de los datos personales en la red, idea que hoy en día es un poco compleja de ejecutar en la práctica.

Cabe señalar que una de las principales normativas que sirvieron para fundamentar uno de los fallos más famosos en esta materia (hablamos de Google contra la Agencia Española de Protección de Datos) fue la directiva 95/46 que había entrado en vigor en el año 1995, estableciendo solamente las condiciones generales de licitud respecto del tratamiento de los datos, por lo que los países miembros de la Unión Europea podían establecer, dentro de estas limitaciones, su propia regulación interna, hecho que refleja la carente y casi nula unificación respecto al tema, sin tener en consideración que las regulaciones existentes no eran acordes a los exponenciales cambios que vive constantemente el mundo de la tecnología. Es por esto que después de dictaminarse el fallo se evidencia la necesidad de crear con urgencia una nueva regulación orgánica que venga a zanjar y solucionar todos estos inconvenientes, es así que en el año 2016 se aprueba el nuevo Reglamento General de Protección de Datos Personales de la UE, el que finalmente en el año 2018 entró en vigencia, siendo de carácter obligatorio para todos los países miembros. Este nuevo reglamento se condice y adapta a las actuales circunstancias, y viene a sentar un modelo y precedente para todos aquellos países que aún no han regulado o actualizado sus legislaciones respectivas en materia de protección de datos personales, para que exista así a nivel mundial ciertos estándares mínimos de protección asegurado a las personas.

Un claro ejemplo de lo anterior es lo que sucede en nuestra propia legislación, ya que en Chile existe una normativa completamente obsoleta en cuanto a la protección de datos personales, puesto que la ley que regula dicha materia es la 19.628, la cual entró en vigencia en el año 1999 y cuyo contenido no es suficiente hoy en día para otorgar la protección necesaria a los ciudadanos respecto del tráfico y tratamiento existente de sus datos personales, por lo que nuestro país se encuentra al debe respecto de este asunto. Un reflejo de la poca eficiencia de esta ley es el hecho de que las personas al momento de buscar protección en el tratamiento de sus datos de carácter personal no recurre al procedimiento estipulado por esta legislación, es decir, no ejercen la acción de Habeas Data contenida en el artículo 16 de la ley 19.628, cuyo procedimiento les resulta un tanto engorroso y tardío, razón por la cual recurren al recurso de protección garantizado en nuestra carta magna, fundamentándolo principalmente en el respeto a la vida privada, la honra de cada individuo y su familia. Cabe mencionar que ni si quiera se le daba carácter de derecho fundamental a la protección de datos, sino que esta debía subsumirse dentro de

los derechos ya mencionados. Frente a esta evidente falta de normativa adecuada y actualizada que ampare a las personas cuyos datos personales son tratados por diversas instituciones, ya sea privadas o públicas, surgen una gran cantidad de proyectos de ley que pretendían modificar tanto la constitución de la republica como la actual ley 19.628, todo esto con la intención de igualar los estándares internacionales, sin embargo, muchos de ellos durmieron por años en el congreso no lográndose concretar ninguno. Esta situación tiene un vuelco recién en el año 2018, ya que se aprueba un proyecto de ley que modifica nuestra carta fundamental, incorporando dentro del catálogo de derechos que protege en su artículo 19 la protección de datos personales, señalando ahora que la constitución asegura "El respeto y protección a la vida privada y a la honra de la persona y su familia, y, asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley". Esto viene a elevar la protección de los datos personales desde un rango legal a un derecho esencial asegurado a todos los ciudadanos del país.

No obstante, y a pesar de este avance en la materia, Chile aún no ha logrado promulgar una ley integral y actual en materia de protección de datos, por lo que sigue encontrándose muy atrasado en comparación a los avances internacionales anteriormente mencionados. Sin embargo, el panorama nacional no resulta del todo desalentador, ya que hoy en día existe un proyecto de ley que se encuentra bien encaminado, nos referimos a fusión de dos boletines realizada el año 2017, a saber, el 11.144-07 y el 11.092. Dicho proyecto de ley se encuentra hoy en día avanzando a pasos agigantados, ya que luego de ser aprobado en general y particular por el senado, en enero de 2020 pasó a segundo trámite constitucional y se encuentra en la cámara de diputados esperando su aprobación para que posteriormente pueda ser promulgada y publicada en el diario oficial, por lo que prontamente podríamos tener un el tan anhelado cambio en nuestra legislación en materia de protección de datos después de más de 20 años.

Bibliografía

- Agencia Española de Protección de Datos. (2014). Conoce la Agencia. De http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/index-ides-idphp.php

- ALEXY, R. (2008). La fórmula del peso. En El principio de proporcionalidad y la interpretación constitucional. Quito: Ministerio de Justicia y de Derechos Humanos.

- Baytelman, Paloma. (2011). Protección de datos personales en la sociedad de redes. En Reflexiones Sobre el Uso y Abuso de los Datos Personales en Chile. Expansiva. De https://www.consejotransparencia.cl/wpcontent/uploads/estudios/2018/01/reflexiones_sobre_el_uso_y_abuso_de_los_datos_personales_en_chile.pdf

- Bembibre, C. (2012). Definición de Banco de Datos. En https://www.definicionabc.com/general/banco-de-datos.php

- Boletín N° 9.384-07. (2014). Proyecto de reforma constitucional, iniciado en moción de los Honorables Senadores señores Harboe, Araya, Lagos, Larraín y Tuma, que consagra el derecho a la protección de los datos personales. En https://senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=9384-07

- Carey, G. & Silva, P.. (2018). Se aprobó en general el proyecto de ley que modifica la Ley de Protección de Datos. En https://www.carey.cl/download/18-05-2018-resumenleyprotecciondatos.pdf

- Directiva 95/46 de la Comunidad Europea. (1995). Del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- European Court of Human Rights. (2010). Convenio Europeo de Derechos Humanos. De Tribunal Europeo de Derechos Humanos. En https://www.echr.coe.int/Documents/Convention_SPA.pdfscielo.org.pe/scielo.php?script=sci_arttext&pid=S1684-09332019000100014.

- EUR- Lex. Protección de los Datos Personales (2015). De http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:l14012

- González Garcés, Miguel. Biblioteca Pública de Coruña. Manual de Internet Avanzado. Disponible en http://rbgalicia.xunta.es/coruna/descargas/1303289914.pdf

- Google. Introducción a los archivos robots.txt. Conceptos básicos sobre los archivos robots.txt: qué son y cómo usarlos. En https://support.google.com/webmasters/answer/6062608?hl=es

- Google, Informática. Datos. En https://sites.google.com/site/informatica123325871/datos

- Instituto Federal de Acceso a la Información Pública de México. (2014). En: http://www.ifai.org.mx/

- JERVIS, Paula. (2003). "Derechos del Titular de Datos y Habeas Data en la Ley 19.628". Revista Chilena de Derecho Informático 2.

- JERVIS, Paula. (2005). "Categorías de datos reconocidas en la Ley 19.628". Revista Chilena de Derecho Informático, Santiago: n° 6.

- Nogueira Alcalá, Humberto. (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". Revista de Derecho de la Universidad Austral de Chile, v.17.

- Quiroz Papa de García, Rosalía. (2016). El Hábeas Data, protección al derecho a la información y a la autodeterminación informativa. Letras (Lima). En http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2071-50722016000200002&lng=es&tlng=es.

- La Constitución de los Estados Unidos de América. (1787). En https://www.archives.gov/espanol/constitucion.

- Ley Nº 19. 628. CHILE. (1999). Sobre protección de la vida privada. Biblioteca del Congreso Nacional de Chile. Ministerio de Secretaría General de la Presidencia.

- Ley N° 21.096. CHILE. (2018). CONSAGRA EL DERECHO A PROTECCIÓN DE LOS DATOS PERSONALES. Biblioteca del Congreso Nacional de Chile. Ministerio de Secretaría General de la Presidencia. En https://www.bcn.cl/leychile/navegar?idNorma=1119730

- MAYOR GÓMEZ, R. (2016). CONTENIDO Y NOVEDADES DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UE (REGLAMENTO UE 2016/679, DE 27 DE ABRIL DE 2016). Gabilex, N°6, De Castilla la Mancha Base de datos.

- Moya, Rodrigo. (1993) La libertad de expresión en la red internet. Revista Chilena de Derecho Informático, Santiago, Chile.

- Palma Pablo. (2015). D° Chile. Sentencia judicial de la C. Suprema en la que obliga a dar de baja fotografía de un grupo de Facebook. En http://www.derecho-chile.cl/sentencia-judicial-facebook/

- Parlamento Europeo y del Consejo. (2016). REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. Diario Oficial de la Unión Europea.

- Parlamento Europeo, el Consejo y la Comisión. (2000). CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA. Diario Oficial de las Comunidades Europeas.

- Pérez Porto, Julián y Merino, María. (2018). Actualizado: 2020. Definicion.de: indexación. En https://definicion.de/indexacion/

- Rodríguez, Rodolfo. (2014). Internet, salud pública 2.0 y complejidad. Revista de la Universidad Industrial de Santander. Salud. En http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-08072014000300010&lng=en&tlng=es.

- ROSEN, J. (2012). The Right to be Forgotten. En http://www.stanfordlawreview.org/online/privacy- paradox/right-to-be-forgotten

- Sandoval, Jessica (2016). EL DERECHO AL OLVIDO. BASES PARA UNA PROPUESTA NORMATIVA EN CHILE. Memoria de prueba para optar al grado de Licenciada en Ciencias Jurídicas y Sociales. Facultad de Derecho. Universidad de Chile.

- Senso, José A., De la Rosa Piñero, Antonio (2003). El concepto de metadato. Algo más que descripción de recursos electrónicos. En http://www.scielo.br/pdf/ci/v32n2/17038.pdf

- Subsecretaría de Telecomunicaciones, Sector de Telecomunicaciones. (2014). Posicionamiento de Chile en Desarrollo Digital Avances. De http://www.subtel.gob.cl/images/stories/apoyo_articulos/notas_prensa/06032014/Informe_Estadistico_SUBTEL_2013.pdf

- Subsecretaría de Telecomunicaciones. (2015). Penetración de Internet en Chile alcanza los 64,2 accesos por cada 100 habitantes. En http://www.subtel.gob.cl/penetracion-de-internet-en-chile-alcanza-los-642-accesos-por-cada-100-habitantes/

- Torres Pombert, Ania. (2003). El uso de los buscadores en Internet. ACIMED. En http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000300004&lng=es&tlng=es.

- Tribunal de Justicia Europeo. En https://www.gmycia.cl/derecho-al-olvido-en-internet

- Tribunal de Justicia de la Unión Europea. (2014). SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala). En http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

- Viollier, Pablo. (2019). El Estado de la Protección de Datos Personales en Chile. Derechos Digitales America Latina. En https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf