UNIVERSIDAD DE VALPARAÍSO
FACULTAD DE DERECHO Y CIENCIAS SOCIALES
ESCUELA DE DERECHO

"El Derecho al olvido: Una mirada desde la protección de datos, legislación comparada, nacional y su procedencia en Chile"

Nombres: Elena Fuentes Villalobos
Mauricio Pérez Tapia

Profesor Guía: Patricia Reyes Olmedo

-2015-

Tabla de Contenidos

Resumen

La sentencia de "Costejo contra Google Inc." del año 2014, que se pronunció en contra de este último, constituye el primer reconocimiento jurisprudencial europeo del derecho al olvido en materia de protección de datos personales.

A lo anterior, se suma la discusión iniciada en el año 2012 en el Consejo Europeo y de la cual emanó el Proyecto de Reglamento de Protección de Datos personales, que lo consagra expresamente.

En los últimos años en Chile también se ha iniciado un debate respecto a la inclusión de este mecanismo y otros, teniendo como marco jurídico la Ley 19.628 de Protección a la Vida Privada que data del año 1999.

Teniendo presente lo anterior, el texto analiza, a la luz de los principios en materia de protección de datos personales y legislación extranjera, la suficiencia o idoneidad de incluir al derecho al olvido en el ordenamiento jurídico nacional.

Palabras claves

Derecho al olvido - protección de datos - proyecto de reglamento de protección de datos personales - Ley 19.628.

I.- Introducción

El auge de las tecnologías de la información de fines del siglo XX, ha generado grandes cambios en las relaciones sociales. El frecuente uso de las distintas redes sociales, la digitalización de los medios de comunicación y de las bases de datos de organismos tanto privados como públicos; además de un acceso expedito y universal a través de herramientas como los motores de búsqueda, han producido una nueva faz de regulación en torno a qué ocurre cuando una persona desea que sus datos personales, dejen de circular en la red.

Esta realidad ha llevado a que hoy en día sea difícil controlar el tratamiento de información y datos personales, lo cual se agrava si tenemos en consideración que con el avance de las tecnologías ya mencionado, el flujo de datos que circulan en el sistema de redes se ha incrementado.

En consecuencia de lo anterior, los ciudadanos han comenzado a recurrir a instancias de tutela para la protección de sus datos personales. Tal es el caso de la sentencia que ha marcado un hito dentro de la materia del derecho al olvido y que fue emitida por la Gran Sala del Tribunal de Justicia Europeo con fecha 13 de Mayo del año 2014 entre las partes, Google Spain, S.L., Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Esta sentencia determinó que Google Inc. vulneró el derecho a la protección de datos personales y el respeto a la vida privada a través del tratamiento de estos datos pertenecientes a Mario Costeja, puesto que permitía que mediante la escritura del nombre del afectado se accediera a todo un listado de enlaces con información relacionada a su persona produciendo afectaciones potenciales en base a sólo el funcionamiento de los motores de búsqueda. Por tanto, toda persona puede oponerse a la indexación de sus datos personales si ello repercute en intromisiones y vulneraciones a su vida privada y datos personales, los cuales forman parte del núcleo del derecho al olvido[1].

[1] La información personal del Sr. Costeja databa de 1998, respecto a un embargo que a ese momento ya se encontraba solucionado y en circunstancias de que se trataba de un aviso en un diario que había sido digitalizado. Revisado en: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES (fecha de última consulta 14 de octubre de 2015)

Así el fallo en cuestión, marca un punto de inflexión en la concepción actual del derecho al olvido, ya que se refirió no sólo a la responsabilidad de quien recopiló los datos sino que también a la del administrador de la búsqueda.

Junto con su contenido mismo, su importancia radica en que ha generado un debate en torno al nivel de protección de datos y al ascenso del derecho al olvido como un mecanismo jurídico más idóneo para proteger los datos personales.

Prueba de ello, es que tras la sentencia– hasta septiembre del presente año – se han presentado cerca de 780 mil solicitudes para eliminar datos personales, como la dirección domiciliaria y de las cuales la mitad han sido acogidas.[2]

Con todo, debido a su carácter contingente y debatido, es que resulta necesario analizar este derecho al olvido y su procedencia dentro de nuestro ordenamiento jurídico nacional.

En esta tesina abordaremos en primer lugar una aproximación al derecho al olvido desde el derecho a la protección de los datos personales, analizando sus principios, presupuestos, para posteriormente analizar el concepto del derecho al olvido.

En segundo lugar, nos referiremos al marco jurídico de la protección de datos tanto a nivel comparado, - como contexto jurídico en que surge el derecho al olvido - específicamente algunos países europeos y otros latinoamericanos y se analizará el instrumento jurídico comunitario que pretende regular el derecho al olvido; el proyecto de reglamento general de protección de datos, para finalmente referirnos al estado actual de la protección de datos en Chile.

Para finalmente, señalar nuestras conclusiones respecto al panorama general del derecho al olvido desde la protección de datos y si es o no procedente el derecho al olvido en Chile, en base a las condiciones analizadas.

[2] El 58,1% de las peticiones han sido rechazadas por no cumplir los criterios. Siendo España el cuarto país con mayor número de solicitudes de borrado en la UE. Revisado en http://www.elmundo.es/tecnologia/2015/05/14/5554546e22601d554a8b456e.html (ultima vez , 14 -10-2015)

II. Aspectos Teóricos

1. Protección de datos

Al comienzo la protección de datos estaba asociado a la privacidad, específicamente hacia fines del siglo XIX en un artículo de la revista de la Universidad de Harvard, se configuró el denominado "derecho a ser dejado solo".

Sin embargo, el año 1983 el Tribunal Constitucional Alemán configura la autodeterminación informativa como un derecho autónomo, lo que ya nos va dando luces del avance en la concepción de asociar los datos con la privacidad a dar autonomía a la protección de los datos. Esto vino a ser ratificado cuando en 1993 el Tribunal Constitucional Español adopta el término de libertad informática.

Posteriormente con la dictación de la Directiva 95/46 de la Comunidad Europea, se busca armonizar las legislaciones nacionales europeas en materia de protección de datos personales.

De esta forma, la protección de los datos personales deja de tener una correspondencia unívoca con el derecho a la vida privada y a la intimidad, para pasar más bien a configurarse como un derecho autónomo relacionado con la posibilidad de cada persona de tutelar la circulación de la información que le incumbe. (Reyes, 2015: p.p. 2-3)

Principios de la protección de datos

Es posible encontrar principios, es decir, ciertos criterios que inspiran, orientan en su interpretación o se pueden convertir en fuente del derecho ante una laguna jurídica para el derecho al olvido que son recogidos principalmente por la doctrina continental europea, los que tienen como fuente las legislaciones nacionales sobre protección de datos y la normativa comunitaria europea en relación al mismo tema.

Así, encontramos el **principio del consentimiento**, que obliga a que: "toda publicación o tratamiento de datos personales sea realizado con el previo e inequívoco consentimiento del afectado" (Hernández, 2013: p. 33), pero, también señala la posibilidad de retractarse, en

cualquier momento, expresando una causa justificada y sin que se le atribuyan efectos retroactivos, como lo contempla la LOPD de España, en su artículo 6.3.

La importancia del consentimiento en cuanto a la publicación de datos personales, no debiere sorprender, ya que estos se encuentran dentro de nuestra esfera de control –lo que la doctrina suele llamar titularidad de los derechos-, ámbito en el cual todos, cada quien como individuo, tiene la posibilidad de decidir respecto a su información personal que se encuentra a disposición del público en general. En esta misma sintonía se encuentra la Directiva 95/46 de la comunidad europea que en su artículo 7° letra A hace alusión a un consentimiento inequívoco del titular de los datos.

Asimismo, este principio está conectado al derecho de oposición del tratamiento de datos personales contemplado en la Directiva 95/46 - texto de referencia en materia de protección de los datos personales de la comunidad europea - pues cuando uno no consiente, o bien, habiendo consentido decide retirar ese consentimiento, entonces se está generando una oposición al tratamiento de tus datos personales, lo que podría producir la eliminación de los datos personales. (De Terwangne, 2012: pp. 59-60).

En nuestra legislación nacional este principio lo encontramos en el artículo 4° de la Ley 19.628 sobre protección de la vida privada, hablando de un consentimiento expreso.

Por otra parte, se encuentra el **principio de finalidad**, conforme al cual, los datos personales son recopilados y tratados para un fin, pero una vez cumplido ese fin, estos datos dejan de ser necesarios y, por tanto, deben ser borrados por el tercero que los tiene bajo su responsabilidad. Tal como lo expresa la LOPD, en su artículo 11.1 al señalar que los datos personales sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con sus funciones, mientras que la misma norma en su artículo 4.5 señala que los datos serán cancelados cuando hayan dejado de ser necesarios o pertinentes para el fin con el cual se recolectaron.

En la misma dirección apunta, De Terwangne al señalar que: *"los datos personales se pueden mantener como tales si la finalidad del tratamiento lo justifica. Se deben hacer anónimos o se deben eliminar una vez que el objetivo se ha logrado o cuando ya no sea necesario mantener el vínculo con personas identificables para lograr ese propósito"* (2012: p. 58).

También menciona una atenuación de este principios, se trata de casos en que se llevan a cabo investigaciones de tipos estadísticas, históricas o científicas, pero con datos que en su inicio, no fueron recopilados para tales fines, por lo que en atención a la importancia social de estos estudios, la Directiva 95/46 contempla la utilización de dichos datos para desarrollar esas investigaciones, pero siempre que se establezcan las garantías apropiadas para tales usos (2012: p. 59,60). En esta misma Directiva, en su artículo N° 6, número 1, letras B y C, se encuentra consagrado este principio en plenitud. En Chile, nuestra Ley N° 19.628 lo recoge en su artículo 9°.

El **Principio de calidad** también adquiere relevancia en cuanto implica que los datos que son tratados, deben ser exactos, veraces y actuales. Lo que en implicaría la imposición de un deber para aquel que realice el tratamiento de los datos. Primero, que se debe asegurar que los datos sean veraces, es decir, que sean verdaderos o que coincidan con la realidad. En segundo lugar, que sean exactos lo que implica que no solo se condigan con la realidad, sino que deben ser precisos, sin errores. Y en tercer lugar, deben ser actuales, o sea, no deben estar desfasados o desactualizados. Este principio está contenido en el artículo 4.3 de la LOPD española, en la Directiva 95/46 en su artículo 6° letra D y en nuestra ley de protección a la vida privada en su artículo 6° y 9° inciso segundo.

El **principio de Seguridad** implica que se deben aplicar todas las medidas, ya sean técnicas, jurídicas, administrativas, entre otras, para evitar cualquier alteración, pérdida, filtración o tratamiento no autorizado de los datos recabados. En vista de los peligros que implica el tratamiento de datos, especialmente en la actualidad y los denominados "ciberataques", es que toma vital relevancia este principio, siendo uno de los pilares fundamentales de la protección de datos. A su vez no solo protege los datos en sí mismos, sino que los posibles derechos que podrían verse afectados por un mal uso de éstos. Esto se encuentra en el artículo 9 de la LOPD ya citada. En la Directiva 95/46 se contempla en su artículo 6° letra E, mientras que en nuestra legislación, la ley N° 19.628 lo contempla en su artículo 11.

Como ya vimos, estos principios también forman parte de los principios generales sobre la protección de datos, entre los que también se encuentran el de *información en la recogida de los datos*, pues no tiene sentido tener un mecanismo de protección, si el titular de los datos no tiene conocimiento del tratamiento de sus datos y el de *secreto o confidencialidad*, que consta en que los

encargados del tratamiento de los datos omitan informar sobre el contenido de los datos (Tabernero, 2014: pp. 6-9)

Derechos Fundamentales Involucrados

No son pocos quienes afirman que consagrar la protección de datos –y establecer el derecho al olvido como un mecanismo jurídico para su efectiva tutela- como un derecho constitucional no tiene mayor sentido, pues si una persona se ve afectado por el tratamiento deficiente de estos, que le genere algún perjuicio o detrimento, entonces se encuentra amparado por los derechos a la intimidad, al honor o a la imagen propia.

Esta última postura fue la sostenida por algunos autores en España, en la instancia de debate sobre el cómo incorporar en su constitución la protección de datos y frente a lo cual, fue el propio Tribunal Constitucional Español, quien se ha dedicado a resolver estas inquietudes. Así, en sentencia 29/2013 con fecha 11 de febrero, dicho tribunal expresa que lo que se intentó realizar al elevar a rango constitucional la protección de datos fue garantizar no solo de manera específica, sino que de la manera más idónea que lo que podían ofrecer los derechos fundamentales de la privacidad, la honra y la imagen propia.

Por consiguiente, es claro que el máximo tribunal español intenta señalar y recalcar que no es un tema de si estos derechos llamados "clásicos" –privacidad, honra e imagen propia- son suficientes o no para proteger los datos personales, más bien declara que, independientemente de aquello, no solo es necesario garantizarlos específica y explícitamente, sino que además hay que dotarlos de mecanismos idóneos para su efectivo ejercicio.

Como señala Hernández, *"el constituyente puso de relieve que era consciente de los riesgos que podrían entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de las personas"* (2013: p. 17).

Incluso el Tribunal Constitucional español, en una sentencia anterior expresó respecto al derecho a la intimidad que:

> *"adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona.*

> *La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención"* (Sentencia 11/1998 de fecha 13 de enero, del Tribunal Constitucional de España).

De esta manera, ambos derechos –tanto el de protección de datos personales como el de la intimidad- tienen un objetivo común, esto es, proteger la vida privada. Sin embargo, tienen una función, un objeto y un contenido distinto.

En cuanto a la función, el derecho a la intimidad tiene por tal proteger frente a la invasión que pueda realizarse a la vida familiar o personal, que una persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad, como expresa la sentencia 144/1999 del 22 de julio, del tribunal Constitucional de España. Mientras que, como señala Hernández "*el derecho fundamental de la protección de datos busca garantizar para el titular de los datos, su control total, ya sea de su uso y destino, para, por ejemplo, impedir su tráfico ilícito y lesivo para la dignidad y otros derechos del titular de los datos"* (2013, p. 18).

Es posible observar la diferencia principal en su función, pues mientras la intimidad consiste esencialmente en una facultad negativa, en donde se busca la no intromisión a mi esfera íntima, el derecho de protección de datos personales posee facultades positivas para un control de los datos, una facultad de disposición sobre mi información personal.

Ahora en cuanto a su *objeto de protección*, hay que destacar que en el caso del derecho a la protección de datos es más amplio, pues abarca no solo a la intimidad en su esfera de protección constitucional, sino que a todos los datos que sean relevantes o tengan incidencia en el ejercicio de cualquier otro derecho de las personas, estén estos presentes en la constitución o no.

Es decir, que la protección de datos al garantizar los datos en sí mismos (pues estos son el bien jurídico), cualquiera sea la vulneración de derechos –constitucionales o no- que su tratamiento produzca, son objeto de protección, no restringiéndose solo al honor, la intimidad o la imagen

propia. Por tanto, la constitucionalización de la protección de datos, permite ampliar el catálogo de posibles afectaciones de derechos y no limitarla a la vulneración de los derechos "clásicos".

Otro punto relevante es el que nos hace ver Hernández señalando que esta protección no solo alcanza a los datos "privados", sino también los públicos que por el hecho de su carácter-ser accesibles al conocimiento de cualquiera- no se encuentran al margen del poder de disposición de estos, porque así lo garantiza el derecho a la protección de datos. Pues, *"de todo esto se deriva que la calificación de "carácter personal" a los datos no quiere decir que solo queden amparados de protección los relativos a la vida privada o íntima de la persona, sino que se protegen todos aquellos que contribuyan a la identificación de la persona"* (2013, p. 19).

En cuanto a su *contenido*, se señala que mientras el derecho a la intimidad impone a los terceros el deber de abstención y no intrusión dentro de su esfera privada y también el no uso o divulgación de lo conocido. El derecho a la protección de datos le atribuye su titular una amplia gama de facultades consistentes en diversos poderes jurídicos, cuyo ejercicio impone a terceros deberes jurídicos que buscan garantizar el control sobre sus datos personales.

Lo esencial es que en el resguardo de la intimidad, se restringe a terceros a inmiscuirse en mi esfera privada o no hacer uso de los datos pertenecientes a dicho ámbito, en tanto, en la protección de datos, se dan variadas facultades para imponer deberes a terceros, que hacen posible un real control de la información de carácter personal. Conforme a esto, es posible sostener que, tal como lo ha sostenido el Tribunal Constitucional español, los derechos a la intimidad, la honra y la imagen propia, si bien pueden ser útiles, no son suficiente, ni menos el instrumento más idóneo para la protección de datos personales.

En Chile no tenemos un derecho a la protección de datos de rango constitucional, por lo tanto, si un individuo se siente afectado con el tratamiento de sus datos personales debe observar el catálogo de derechos contenidos en el artículo 19 de la Constitución Política e intentar demostrar que el tratamiento de datos vulneró al menos uno de los derechos contenidos en dicho catálogo.

Es posible decir que la concepción de nuestra legislación no es de proteger los datos como tales, sino solo los derechos garantizados en la constitución. Podríamos hablar de una

protección indirecta, pues se protegen los datos siempre que se haya afectado un derecho. Lo anterior marca una diferencia de fondo en relación con Europa, pues mediante la legislación comunitaria e interna ellos han constitucionalizado la protección de datos logrando así proteger los datos personales por el solo hecho de configurarse como tal.

Todo lo indicado queda en evidencia en el título de nuestra normativa, pues en nuestra Ley 19.628 se titula "sobre la protección de la vida privada", lo que nos lleva a estar más cerca de los derechos incluidos en el catálogo del artículo 19 de la Constitución Política como la honra o la intimidad, que a poder constituir un derecho a la protección de datos personales como tal.

2. Derecho al olvido

¿Qué entendemos por derecho al olvido?

Desde sus orígenes, qué se debe entender por derecho al olvido, ha sido un tema controvertido, que ha derivado en múltiples pugnas, tanto en algunos Estados, como entre gran parte de la doctrina, lo cual deriva en una falta de concepto oficial, ya que se ha privilegiado el análisis fáctico en desmedro de lo conceptual.

Así los autores que se han expuesto sus argumentos en favor o en contra de este derecho, lo hacen sin detenerse siquiera en explicar qué entienden por derecho al olvido (Abril y Pizarro, 2014: p. 24).

Sin perjuicio de lo anterior, es posible encontrar algunas situaciones –particularmente en sus orígenes- en donde se asocia el concepto de derecho al olvido al silenciar eventos pasados de la vida que ya no están sucediendo (Cortés, 2012: p. 15), lo que nos da algunas luces sobre las primeras nociones de este derecho; primero el "silenciar" lo que se podría asemejar al borrar o eliminar; segundo, los "eventos pasados" que se podría asociar a la información que se quiere eliminar o borrar y tercero, "que ya no están pasando", lo que nos impondría una condición, esto es, que los eventos pasados que se pretenden silenciar, hayan mutado.

A este respecto, es importante señalar lo propuesto por la abogada belga, experta en derechos humanos y protección de datos, Cecile De Terwangne, para la cual: *"es el derecho de las personas*

físicas a hacer que se borre la información sobre ellas después de un período de tiempo determinado" (2012: p. 54).

Hoy en día, el concepto se ha perfeccionado, incluso haciendo algunas distinciones necesarias de mencionar. Pues se proponen dos conceptos distintos de derecho al olvido.

El primero hace referencia a las concepciones iniciales de este derecho que se enfocaba en el aspecto comercial o crediticio, dando cuenta de los registros de morosidad o de deudores. Se le denomina olvido de las informaciones crediticias adversas, cuya procedencia está vinculada al paso de un transcurso de tiempo, que varía según cada legislación.

En cuanto al segundo, se trata de un *derecho a la supresión de determinados datos personales* que ya no son necesarios para la finalidad por la que fueron tratados o por el tiempo transcurrido o por ser inapropiados, irrelevantes o desactualizados, y siempre que no exista interés público basado en el derecho a la libertad de expresión, en que sigan siendo conservados (Fernández, 2015: p. 4). En este último, surge algo relevante, esto es, que existen situaciones excepcionales en donde al existir un interés público comprometido cuya fuente sean derechos fundamentales, entonces no sería procedente el derecho al olvido. Esto sin perjuicio de otras excepciones que se analizarán en su momento.

Ya habiendo expuesto varios conceptos, creemos que es pertinente crear uno propio y caracterizarlo.

Así podemos decir que el derecho al olvido es un mecanismo jurídico que se manifiesta en la facultad que tiene toda persona natural, de solicitar a la autoridad competente, que ordene la eliminación y/o desindexación de datos o información, de carácter personal, al responsable de su tratamiento, por haber una falta de consentimiento o un retracto en el consentimiento entregado por el titular del derecho, cuando ya se hayan cumplido los fines para los que fueron recopilados, cuando los datos fueren inexactos, falaces o desactualizados o cuando no se hayan resguardado diligentemente los datos almacenados.

Primero podemos sostener que es un mecanismo jurídico pues es un modo de accionar el derecho ante el acaecimiento de un hecho. Y esta puesta en marcha está representada en una facultad que tendría un titular de los datos, pues al ser una facultad, da lugar a la discreción que tendría este titular de accionar o no este mecanismo.

En segundo lugar, el titular de este derecho sería una persona natural. Se excluye a las personas jurídicas debido a que en general se ha entendido que éstas disponen de más medios para asegurar sus datos, en comparación a una persona natural. Además, debido a su posición y relevancia pública sus datos son de interés público y si en caso de afectar derechos fundamentales pueden recurrir mediante los procedimientos de tutela basados en derechos tales como la honra y la imagen, entre otros.

Así también se ha entendido en la comunidad europea, pues tanto en la Directiva 95/46 como en el proyecto de reglamento europeo sobre protección de datos se ha entendido que este derecho estaría circunscrito a las personas físicas o naturales.

Ahora, la solicitud se debe realizar a una autoridad que tenga la competencia en el asunto, denominado órgano garante. En este caso hay que observar lo que disponga cada legislador, sin embargo, en general la primera reclamación, antes de acudir a un tribunal, se realiza ante una agencia o servicio público especializado en el tema. Así por nombrar un solo ejemplo, en España existe la Agencia Española de Protección de Datos.

Este órgano garante –en caso de acoger la petición- ordenará la eliminación y/o desindexación[3] de los datos en personales debido a que no siempre basta con la sola eliminación de la información, como por ejemplo en aquella situación en que se borran los datos, pero en los motores de búsqueda –al estar esto indexados- siguen encontrándose referencias a la información que fue borrada.

Esto plantearía la necesidad de eliminar la información, pero además ordenar su desindexación para que de esa forma los motores de búsqueda lo borren de sus índices.

Está de más decir que esto quedaría a voluntad del solicitante, pues si para él basta con la eliminación, entonces puede solicitar solo esto, sino puede pedir además la desindexación.

En cuanto a que los datos sean de carácter personal hay que observar lo que se entiende por ello: información concerniente a personas naturales, identificadas o identificables. Así al menos lo contempla la ley N° 19.628 sobre protección de la vida privada, en su artículo 2° letra F.

[3] La indexación es un modo de administrar una base de datos y consiste en realizar índices para agilizar la búsqueda de información. Así, la desindexación consiste en la eliminación de información de los índices respectivos, es decir, la eliminación de los enlaces desde los buscadores.

Básicamente lo mismo dice la LOPD española en su artículo 3°, letra A. Mientras que más exhaustiva es la Directiva 95/46 pues señala en su artículo 2°, letra A: "datos personales son toda información sobre una persona física identificada o identificable (el interesado); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

La orden de eliminar y/o desindexar la información, va dirigida a quien realizó el tratamiento de los datos. En relación a esto, nos parece adecuada la definición de tratamiento de datos que nos otorga la Directiva, en el mismo artículo, pero en su letra B: "Tratamiento de datos personales es cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción".

Ahora en cuanto a las causales por las que procedería este derecho, básicamente se hace referencia a los principios de la protección de datos que se señalaron precedentemente, y que informan y configuran el derecho al olvido. El que haya una falta de consentimiento o un retracto en el consentimiento entregado por el titular del derecho dice relación con el principio del consentimiento, el que se hayan cumplido los fines para los que fueron recopilados es la manifestación del principio de finalidad, cuando los datos fueren inexactos, falaces o desactualizados es expresión del principio de calidad o cuando no se hayan resguardado diligentemente los datos almacenados se vincula con el principio de seguridad.

Esto ya fue analizado con mayor profundidad en su momento, por lo cual no ahondaremos mucho más en este tema, salvo para dejar en evidencia la relación clara entre las causales y los principios de la protección de datos.

Presupuestos

Junto con reconocer un concepto de derecho al olvido también es necesario tener presente ciertos presupuestos para que el derecho al olvido se configure, entendiendo por presupuestos aquellas situaciones fácticas que deben darse para que proceda el derecho al olvido.

En primer lugar, se requiere la *existencia de datos personales*, pues estos son el objeto de protección del derecho al olvido (Tabernero, 2014: p. 14). Si bien existen diferencias en cuanto a la concepción de éstos, en general, las normas legales de los distintos Estados son bastante similares –se diferencian básicamente en la forma en que se les protege - ya que, por ejemplo en nuestro país, la ley 19.628 sobre protección de la vida privada nos indica en su artículo 2, letra f, qué se entiende por datos personales, siendo estos "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables".

En segundo lugar, es necesario el conocimiento de que los datos personales están siendo tratados, y a su vez, cuales datos personales están siendo tratados, lo que es llamado por Tabernero como facultades accesorias de *accesibilidad de los datos* y la de *información del tratamiento realizado* (2014: p. 14). Esto es crucial, pues si el titular de los datos no tiene conocimiento sobre estos puntos, poco o nada puede hacer, a pesar de tener los mecanismos jurídicos que lo protejan. Además, también se encuentra íntimamente ligada a la facultad de autocontrol- que consiste en que el hecho de ceder los datos a un tercero, no supone la renuncia a la titularidad de esos datos, debiendo ese tercero mantener informado sobre el tratamiento de los datos y que los datos le sean accesible al titular de los mismos (Tabernero, 2014: p. 15).

En tercer lugar, que el titular de los datos sea una persona natural[4], lo que ya fue analizado a propósito de la definición del derecho al olvido.

[4] Es necesario hacer presente que en el contexto continental europeo se habla de "persona física", sin embargo, en nuestra legislación nacional se habla de persona natural, siendo ambas para estos efectos, lo mismo.

III. Marco Jurídico Derecho al Olvido: derecho extranjero y nacional.

1. Derecho Extranjero

A. Europa

La inquietud por el tratamiento de los datos personales tiene su origen en el continente europeo. Allí, se configuró a partir de instrumentos normativos, sin fuerza vinculante, hasta finalmente constituir una legislación comunitaria que dio pauta para las legislaciones nacionales europeas.

Conforme a este marco jurídico, el derecho al olvido ha comenzado a configurarse de manera autónoma.

A.1 Nivel Comunitario

La primera iniciativa formal se materializa en el denominado "**Convenio 108**" del año 1981, cuyo objeto fue el tratamiento automatizado de los datos personales, el cual fundó la protección de los datos en el respeto de las garantías fundamentales; agregó la categoría de datos sensibles y señaló los principios en esta materia que acompañan al derecho hasta el día de hoy.

No obstante, el instrumento jurídico que sentaría un paradigma internacional en materia de protección de datos sería la "**Directiva 46/95/C5**", del año 1995, que "*Sienta las bases para lograr la coordinación de las legislaciones nacionales aplicables en materia de protección de datos"* (Bru, Elisenda: 2007, p 64), el cual aportó la obligación de cumplir un nivel adecuado de protección, agregando, además, normas de conflicto para dirimir pugnas interestatales, sistematizando los principios aportados por el Convenio 108, otorgando especial énfasis al "principio de consentimiento"-aunque con importantes excepciones-, circunscribiendo la legitimidad del tratamiento al "principio de finalidad" (Cerda, Alberto: 2003, p. 54).

Con todo, no fue sino hasta el 4 de Noviembre del año 2010 que la Comisión Europea emite una comunicación a sus Estados Miembros, durante la revisión de la Directiva, en la cual señaló:

> *"Para garantizar que los ciudadanos gocen de un elevado nivel de protección de datos, deben cumplirse dos condiciones previas: el tratamiento de los datos por los responsables del tratamiento debe limitarse únicamente a su propósito (principio de minimización de los datos) y los interesados deben conservar un control efectivo sobre sus propios datos"* (Comunicación de la CE al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones, COM: 2010, p.3).

Junto con señalar los lineamientos que han de seguir los Estados miembros en materia de protección de datos, la Comisión entrega un aporte histórico para el desarrollo del derecho al olvido, pues presenta el primer concepto de éste y con ello su primer reconocimiento formal, definiéndolo como:

> "*The right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes*", es decir, el derecho que los individuos tienen a que sus datos dejen de ser tratados y sean eliminados cuando han dejado de ser necesarios para fines legítimos (Comunicación de la CE al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones, COM: 2010, p.8).

Cabe mencionar que para la Comisión no se trataría de un derecho del todo nuevo, si no que deriva de los denominados "Derechos ARCO", un acrónimo de los siguientes derechos, a saber: acceso, derecho a solicitar información al responsable del registro de datos respecto a si su datos personales están siendo tratados y de ser así, con qué finalidad, su origen y difusión; rectificación, solicitud de modificar los datos por incompletos o inexactos; oposición, a que no se practique el tratamiento a los datos personales o a que se le ponga fin en caso que en principio no haya sido necesario el consentimiento, en los casos que el registro se utilice para fines publicitarios o para la adopción de una decisión que afecte al interesado y cancelación, conforme al cual el afectado puede solicitar la supresión de aquellos datos que sean inadecuados o excesivos, sin perjuicio del bloqueo que debe practicarse[5]. Pero en vista de que

[5] https://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/index-ides-idphp.php. (Fecha última consulta 20/10/2015)

no existe un nivel adecuado de protección de datos, se requiere de un mecanismo de mayor idoneidad y eficiencia.

En reflejo de lo anterior, a inicios del año 2012 la Comunidad Europea propone un Proyecto de Reglamento General de Protección de Datos[6], que reemplazará a la Directiva y en la que se reconoce de manera expresa, en el artículo 17, el derecho al olvido.

De acuerdo a este Reglamento, *"la desigual manera de enfrentar los riesgos causados por el fenómeno de Internet de las distintas legislaciones de los Estados miembros ha dado lugar a una inseguridad jurídica en materia de protección de datos"* (Tabernero, Silvia: 2014, p.20).

Este Reglamento, en sus primeros artículos, delimita ciertos puntos: a) Que su ámbito de aplicación se encuentra circunscrito a la Unión Europea, b) su objeto material excluye a los datos personales que sean familiares o domésticos; pero sí debe aplicarse a los responsables que proporcionen los medios para el tratamiento de éstos; y c) serán legitimados para invocarlo las personas físicas; excluyendo a las personas jurídicas.

Ahora bien, al respecto cabe efectuar algunos comentarios en relación a aspectos que no resultan obvios; la legitimación por parte de las personas físicas en desmedro de las personas jurídicas, con ello no es que se pretenda señalar que las personas jurídicas no cuentan con datos personales que fundamente su acceso en principio a los derechos ARCO y consiguientemente al derecho al olvido, sino que debido a su posición y relevancia pública sus datos son de interés público y si se sobrepasa dicho umbral, cabe que recurran a los procedimientos de tutela basados en derechos tales como la honra y la imagen.

Por otra parte, la exclusión de los datos personales domésticos o familiares también se entiende, puesto que se encuentran circunscritos al ámbito personal, esfera en que el titular de los datos personales tiene pleno dominio; no ocurriendo así en caso que se difundan o reproduzcan fuera de esos límites, momento en el cual el Reglamento será aplicable. Advirtiéndose a primera vista que muchas veces las fronteras entre lo personal y lo público se

[6] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, (COM/2012) 11 finales, de 25 de enero de 2012, puede consultarse en: http://eurlex. europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF

encuentran difusas y deberá ser analizado caso por caso. Al respecto, la Agencia Española de Protección de Datos en informe emitido el año 2008, ha adoptado el criterio señalado por los tribunales españoles, manifestado: "*Será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos*"[7].

Ya en el análisis de fondo del derecho al olvido, el artículo 17 apartado 1 comienza señalando:

> *"El interesado tendrá derecho a que el responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de darles más difusión y, en relación con terceros, a que éstos supriman todos los enlaces a los datos personales, copias o reproducciones de los mismos, cuando concurra alguna de las circunstancias siguientes:*
>
> *a) los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados;*
>
> *b) el interesado retira el consentimiento en que se basa el tratamiento de conformidad con lo dispuesto en el artículo 6, apartado 1, letra a), o ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos;*
>
> *c) el interesado se opone al tratamiento de datos personales con arreglo a lo dispuesto en el artículo 19;*
>
> *d) el tratamiento no es conforme con el presente Reglamento por otros motivos."*

Así, lo primero que se observa es que el derecho al olvido supera a la protección promovida a través del ejercicio de los derechos ARCO, ya que también tiene en cuenta la vigencia ulterior de aquellos datos personales debido a la acción del responsable de ellos, es decir, se encuentra *"estrechamente vinculado con las facultades de supresión de los datos personales aunque también integra la capacidad de exigir al responsable del tratamiento que se abstenga de darles mayor difusión" (Gallardo, Marc: 2014, p. 3).*

[7] En Informe 007/2013 de la Agencia Española de Protección de datos, sentencia de la Audiencia Nacional 16 de Junio de 2006. Revisado en https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2008-0615_Inaplicaci-oo-n-LOPD-a-actividad-de-particulares-que-comparten-fotos-de-sus-hijos-a-trav-ee-s-de-Internet.pdf Fecha última consulta 20/10/2015

Pero este proyecto no sólo aporta en términos de consagración el derecho al olvido como tal, con una gran trascendencia al debate también se refiere al responsable del tratamiento de los datos –o encargados quienes actúan bajo su mandato, y al consentimiento.

El Reglamento ha cambiado la dirección hacia quien tiene la responsabilidad respecto de los datos personales , así *"Frente a quienes han mantenido que el derecho al olvido en Internet debía pivotar sobre el derecho de oposición ejercido sobre los motores de búsqueda como responsables de sus propios tratamientos –la sentencia contra Google Inc. desarrolla su argumentación sobre la responsabilidad del buscador –, la propuesta de Reglamento construye el derecho al olvido en Internet sobre las obligaciones del responsable principal –de la web máster– que ha hecho público los datos.* (Troncoso, Antonio: 2010, pp. 816-831).

Al respecto, el aparto 2 del Proyecto señala que:

> *"Cuando el responsable del tratamiento contemplado en el apartado 1 haya hecho público los datos personales, adoptará todas las medidas razonables, incluidas medidas técnicas, en lo que respecta a los datos cuya publicación sea responsable con miras a informar a los terceros que están tratando dichos datos de que un interesado les solicita que supriman cualquier enlace a esos datos personales o cualquier réplica o copia de los mismos. Cuando el responsable del tratamiento haya autorizado a un tercero a publicar datos personales, será considerado responsable de esa publicación."*

En cuanto al consentimiento, señala que este debe ser explícito y que se materializa a través de una declaración o una acción afirmativa, lo cual tiene impacto, "*teniendo en cuenta que una de las circunstancias en las que el derecho al olvido es ejercido es la revocación del consentimiento; influye en que la carga de la prueba del consentimiento pase a recaer en el responsable del tratamiento y porque el consentimiento es necesario para aceptar la política de privacidad de todos los prestadores de servicios de Internet, que normalmente viene establecida por defecto una vez que se consiente en ceder los datos para su tratamiento y recibir la prestación del servicio.*" (Tabernero, Silvia: 2014, p. 24).

La importancia del consentimiento, radica en que se trata tanto del sustento que legitima el tratamiento de los datos personales como aquel que pone fin al mismo, de modo que su carácter explícito permite determinar clara e indubitadamente cuándo se está permitido

recopilar datos personales y cuándo caduca dicha posibilidad, ya que proviene de actos concretos como una declaración o acción afirmativa.

Siendo posible afirmar que "*estos motivos vinculan estrechamente las causas del ejercicio del derecho al olvido con los principios tradicionales del derecho a la protección de datos: principio de licitud del tratamiento, consentimiento y finalidad, así como los derechos de cancelación, revocación del consentimiento y oposición*" Gallardo, Marc: 2014, p. 4).

Con todo, el derecho al olvido no se encuentra consagrado en términos absolutos, ya que cuenta con excepciones vinculadas a los fines que motivaron la recopilación de aquellos datos personales, como lo presenta el Reglamento en su apartado 3:

"*El responsable del tratamiento procederá a la supresión sin demora, salvo en la medida en que la conservación de los datos personales sea necesaria:*

a) para el ejercicio del derecho a la libertad de expresión de conformidad con lo dispuesto en el artículo 80;

b) por motivos de interés público en el ámbito de la salud pública de conformidad con lo dispuesto en el artículo 81;

c) con fines de investigación histórica, estadística y científica de conformidad con lo dispuesto en el artículo 83;

d) para el cumplimiento de una obligación legal de conservar los datos personales impuesta por el Derecho de la Unión o por la legislación de un Estado miembro a la que esté sujeto el responsable del tratamiento; las legislaciones de los Estados miembros deberán perseguir un objetivo de interés público, respetar la esencia del derecho a la protección de datos personales y ser proporcionales a la finalidad legítima perseguida;

e) en los casos contemplados en el apartado 4.

Estas limitaciones se fundamentan en palabras del propio Consejo en que *"El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función*

en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad".[8]

De modo que las solicitudes y controversias que traigan consigo, deberán ser analizadas caso a caso por las autoridades en materia de protección de datos y los tribunales, lo cual no será fácil de resolver, especialmente respecto a la causal letra a), pues la libertad de expresión se ha convertido en una consignas de la era de las comunicaciones.

Sin perjuicio de lo anterior, en su apartado 5 también expresa causales conforme a las cuales se atenúa el derecho al olvido:

"*En lugar de proceder a la supresión, el responsable del tratamiento limitará el tratamiento de datos personales cuando:*

a) el interesado impugne su exactitud, durante un plazo que permita al responsable del tratamiento verificar la exactitud de los datos;

b) el responsable del tratamiento ya no necesite los datos personales para la realización de su misión, pero estos deban conservarse a efectos probatorios;

c) el tratamiento sea ilícito y el interesado se oponga a su supresión y solicite en su lugar la limitación de su uso;

d) El interesado solicite la transmisión de los datos personales a otro sistema de tratamiento automatizado de conformidad".

El apartado hace pensar en el uso de medidas ya existentes en el mundo de la web, pero que se descartan por ser insuficientes en sí mismas, como la anonimización[9], pues si bien permite que, mientras se esté evaluando la ulterior supresión de los datos personales, no estén asociados a la personas física a la cual aluden- pues sólo se usarán iniciales en vez del nombre completo- nada asegura la imposibilidad de acceder a la información a través de otros nombres que figuren en

[8] De acuerdo al informe interinstitucional de la Propuesta de Reglamento del Parlamento Europeo y del Consejo que señala las cuestiones preliminares que llevaron a la presentación de este nuevo cuerpo normativo. Revisado en http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/es/pdf

[9] A la luz de la Directiva 95/46/CE es posible definirla como la eliminación de los elementos suficientes de modo tal, que mediante el conjunto de los medios que razonablemente se utilizan, no pueda identificarse al interesado. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf

el mismo tratamiento de datos, por lo que resulta insuficiente de manera aislada; aunque sí resultaría idónea para una limitación de carácter temporal, como las señaladas en este apartado.

Ahora bien, estos preceptos serían meras declaraciones si no fuera por las condiciones de garantía de este derecho al olvido, que constituyen pautas de control permanente del tratamiento que se puede estar confiriendo a datos personales.

En efecto, en el apartado 6 el Reglamento expresa que: "*El responsable del tratamiento implementará mecanismos para garantizar que se respetan los plazos fijados para la supresión de datos personales y/o para el examen periódico de la necesidad de conservar los datos*".

Agrega el apartado 7 que *"Cuando se hayan suprimido datos, el responsable del tratamiento no someterá dichos datos personales a ninguna otra forma de tratamiento."*

Y finalmente, el apartado 9 señala "*La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar*:

a) los criterios y requisitos relativos a la aplicación del apartado 1 en sectores y situaciones específicos de tratamiento de datos;

b) las condiciones para la supresión de enlaces, copias o réplicas de datos personales procedentes de servicios de comunicación accesibles al público a que se refiere el apartado 2;

c) los criterios y condiciones para limitar el tratamiento de datos personales contemplados en el apartado 4.

En cuanto a su discusión, luego de tres años el 15 de junio del presente año, el Consejo Europeo llegó a una orientación general que consiste en un acuerdo político sobre el cual se puede iniciar las negociaciones con el Parlamento Europeo.[10]

A.2 Nivel Interno

A nivel local, gracias a la influencia de los mencionados instrumentos jurídicos, la obligación de generar sus propios sistemas de protección de datos personales fue interiorizándose en los países miembros.

[10] http://www.consilium.europa.eu/es/press/press-releases/2015/06/15-jha-data-protection/

El caso de España en que existe un reconocimiento constitucional a través del derecho a la intimidad, pero que se proyectó legalmente a través de la Ley Orgánica de Protección de Datos de Carácter Personal del año 1999, que manifiesta que los datos personales se encuentran sujetos a un plazo de caducidad, dado por la necesidad o la pertinencia que motivó que fueran recopilados o registrados, es decir, se prohíbe la perpetuación del tratamiento de los datos personales cumplida su finalidad.

A nivel jurisprudencial, como hemos visto, el propio Tribunal Constitucional Español ha reconocido un derecho a los datos personales. A partir de este reconocimiento se proyectaría también el derecho al olvido.

En sus propias palabras:

> *"este poder de control y disposición, concretado en una serie de facultades de su titular como consentir la recogida y el uso de sus datos personales, conocer los mismos, ser informado de quién los posee y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo que ponga fin a la posesión y empleo de tales datos, constituyen el contenido esencial del derecho a la protección de datos de carácter personal*" (STC 290/2000, de 30 de noviembre, FJ 7).

Así, para velar por el cumplimiento de estos preceptos, se crea la "Agenda Española de Protección de Datos", que se ha pronunciado de modo fructífero, puesto que se trata de un órgano que se ha convertido en eficiente protector de los datos personales.

La doctrina se refiere a su labor con el derecho al olvido, destacando que "*ha atribuido una extensión notable al derecho al olvido, entendiendo que los ciudadanos, de un lado, pueden ejercer el derecho de cancelación de los datos que la red conserva cuando estos no se contengan en una fuente accesible al público ni exista una finalidad legítima que proteja la publicación*" (Castellano, Simón: 2012, p.4).

En consecuencia, la persona cuenta con una serie de facultades basadas en el poder de disposición de sus datos personales, a saber; el derecho de modificación, oposición y cancelación, los cuales –de conformidad a la sentencia del Tribunal de Justicia de la Unión Europea de 13 de Mayo del año 2014, no son otra cosa que derecho al olvido.

Por su parte, de manera similar, otros países miembros de la UE han formularon sus propias leyes y para promover su eficacia, también han creado órganos especializados desconcentrados.

Tal es el caso de **Alemania**, que tras un desarrollo jurisprudencial de hace un par de década culmina dicho proceso con su Ley Federal de Protección de Datos de 2001 y el "*Comisionado Federal para la Protección de Datos*"; **Italia** con su Código en materia de protección de los datos personales de 2003 y su "*Garante para la Protección de Datos Personales*"; y **Francia**, con su "*Commission Nationale de l'Informatique et des Libertés*" traducido como la "*Comisión Nacional de Informática y Libertades*" (CINL), que al igual que Alemania cuenta con un vasto debate sobre protección de datos personales, siendo un país activo en la defensa y promoción del derecho al olvido como un mecanismo necesario a nivel mundial, siendo una manifestación de ello la multa que la Comisión impuso a Google Inc. por no ajustar sus protocolos de almacenamiento y seguimiento de las legislaciones internas.[11]

No por nada dichos países han presentado mayor cantidad de solicitudes de derecho al olvido, reflejando con ello la mayor cultura jurídica que poseen en materia de protección de datos[12].

B) Latinoamérica

A diferencia de Europa, Latinoamérica no cuenta con un histórico debate en materia de protección de datos, principalmente porque la tecnología ha penetrado con mayor tardanza en la región y la protección de datos constituye una reacción frente al tratamiento automatizado, que aún no era una realidad latinoamericana.[13]

---

[11] La CNIL ha cuestionado la decisión del buscador de fusionar en una sola política las diferentes reglas de confidencialidad aplicables a servicios como YouTube, Gmail o Google Maps, entre otros, pues si bien entiende la simplificación de protocolos y no cuestiona su legitimidad, considera que es contario a los requerimientos legales, pues no se informa de manera suficiente. http://www.europapress.es/portaltic/empresas/noticia-francia-multa-google-incumplir-ley-proteccion-datos-20140108225421.html. Fecha de última consulta 20/10/2015.

[12] Conforme a los datos entregados por Google, Francia es el país de la Unión Europea con más peticiones, con 52.136, seguido de Alemania con 43.366 y España con 23.524. De las cuales , Google ha rechazo un 59% de todas las solicitudes presentadas http://es.engadget.com/2015/05/14/google-rechaza-el-59-de-las-peticiones-al-derecho-al-olvido . Fecha última consulta 20/10/2015.

[13] Artemi Rallo *el at*, .(2012) en Curso "El derecho a la protección de datos" Capítulo 6: La protección de datos y el habeas data en Latinoamérica.3era edición Fundación CEDDET, Madrid, España.

Sin embargo, a partir de la última década, algunos países se han visto influenciados por las tendencias europeas- Directiva y el caso español- comenzado a formular sus propias regulaciones.

En México, cuentan con una Ley Federal de Protección de Datos Personales en Posesión de los particulares del año 2010 y que entró en vigencia el año 2012. Ésta prescribe, en su artículo 1°, que el responsable de los datos personales debe velar porque éstos se encuentren en un estado idóneo para el fin por el cual fueron recopilados, en orden a que se encuentren actualizados y pertinentes. Por consiguiente, una vez caducado el uso de aquellos datos, éstos han de ser cancelados.

Al respecto, la ley establece un plazo general relacionado a la vigencia de la finalidad por la que los datos fueron recabados y un plazo especial respecto de obligaciones comerciales, de 6 años.

Pese a ser una de las legislaciones más jóvenes de nuestro continente, ha sentado el primer antecedente latinoamericano a través de la acción del Instituto Federal de Acceso a la Información, que modificó recientemente su nombre a Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). El INAI a principios de este año inició un procedimiento en contra de Google México –de modo similar al caso Español, por no atender la solicitud de un empresario que se encontraba disconforme con el tratamiento de sus datos en el servicio de motor de búsqueda. Conforme a una información publicada, un empresario transportista habría donado aulas móviles a la fundación de la esposa del expresidente Vicente Fox, por lo cual –independiente de su veracidad o no, pretendía que se borrara del motor de búsqueda. Sin embargo, Google México no atendió la solicitud, ya que señaló que es Google Inc., ubicada en Estados Unidos, la encargada del motor de búsqueda, por lo que Google México no era responsable de dicho tratamiento de datos; frente a lo cual se determinó que "*Google México, se trata de una empresa legalmente constituida en México por tanto, en los términos de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares es responsable del tratamiento de datos personales*"[14].

[14] Hechos y argumentos revisados en http://inicio.ifai.org.mx/pdf/resoluciones/2014/PPD%2094.pdf

En América del Sur, Uruguay ha sido reconocido por la Comunidad Europea como un país con un nivel adecuado de protección[15], gracias a la Ley 18.331 sobre Protección de Datos Personales del año 2008, cuyo ámbito material recae en cualquier tipo de tratamiento de los datos personales y al sujeto pasivo de éstos, es decir, proveniente de un tratamiento automático o manual y ya sea de una persona natural como jurídica, lo que la destaca respecto de legislaciones europeas, pues como se analizó previamente las personas jurídicas se encuentran excluidas.

De igual modo que las legislaciones comentadas, en su artículo 8 advierte la relación entre datos personales y la vigencia del motivo por el cual fueron recopilados, es decir, principio de finalidad. Mientras que en materia sustancial, presenta un catálogo de derechos entre los cuales se encuentran la cancelación, supresión u oposición, facultades que como ya se ha presentado, son instrumentales al derecho al olvido, operando bajo los siguientes supuestos: solicitud de cancelación cuando a partir del tratamiento de los datos personales se genere perjuicios a los derechos e intereses de terceros, sea información errónea; o contravenga lo señalado por la ley.[16]

Por otro lado, para velar por el cumplimiento del sistema de protección, crea la "*Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento*" (AGESIC), cuyo órgano de control de la aplicación de la legislación de protección de datos y el respeto a los principios es la Unidad Reguladora y de Control de Datos Personales. Conjuntamente con Uruguay, se destaca el caso de Argentina que posee la Ley 25326 acompañada del Decreto Ley 1558/2001, y que fue el primer país latinoamericano al cual la Comunidad Europea señaló como adecuado en materia de protección de datos.

De igual modo el marco normativo argentino, arguye que el tratamiento de los datos personales, se encuentra vinculado a la vigencia del fin por el cual se recopilaron, así como

[15] Se trata de un reconocimiento a Uruguay, como país en condiciones de asumir el desafío de cumplir con los controles que exige la Unión Europea en el uso de los datos personales y a la tarea realizada por la Unidad Reguladora y de Control de Datos Personales (URCDP), ya que favorece el flujo de datos y la transferencia de información. – En http://datospersonales.gub.uy/inicio/institucional/noticias/uruguay-pais-adecuado-en+proteccion-de-datos

[16] En " Aproximaciones al derecho al olvido" informe de la AGESIC, revisado en http://www.agesic.gub.uy/innovaportal/file/3549/1/derecho_al_olvido.pdf fecha última consulta 14/11/2015.

también establece plazos especiales en materia de interés comercial , prevé un habeas data y creó su órgano de control; la Dirección Nacional de Protección de Datos Personales.

Este órgano garante, que cuenta con una destacada labor jurisprudencial, ha consagrado de modo expreso el derecho al olvido, expresando en un fallo histórico de fecha 12 de noviembre de 1999:

> "*Existe asimismo un "derecho al olvido". Este es, el principio a tenor del cual ciertas informaciones (vgr. antecedentes penales prescriptos) deben ser eliminados de los archivos transcurrido un determinado espacio de tiempo desde el momento en que acaeció el hecho a que se refieren, para evitar que el individuo quede prisionero de su pasado".*

2. Derecho Nacional

Chile a diferencia de los países latinoamericanos mencionados en párrafos anteriores, tiene una deuda pendiente en materia de protección de datos, razón por la que no forma parte de los países considerados con un nivel adecuado de protección.

Ahora bien, lo señalado no sólo alude al aspecto jurídico sino que también es posible extrapolarlo a la educación en esta materia ya que "*una sociedad conectada en red requiere de políticas de alfabetización digital que consideren de una parte las destrezas necesarias para el manejo de los sistemas de información y de otra, la formación de una cultura digital que permee en todas las capas sociales y les permita a las personas conocer e internalizar no sólo funcionamiento técnico sino que las implicancias del desenvolvimiento en la nueva sociedad*" (Donoso, Lorena: 2013, p. 95).

Por otra parte, si bien Chile no ha reconocido la libertad informática o la autodeterminación informativa como un derecho fundamental, luego de un largo proceso legislativo que se inició en 1984, el 28 de Agosto de 1999 se publicó en el Diario Oficial la Ley 19.628, bajo el título "*Ley sobre protección de la vida privada*", pero que respondería mejor al título "*Regulación del Tratamiento de Datos Personales*" (Donoso, Lorena: 2013, p. 91), siendo una de las primeras legislaciones en la materia a nivel latinoamericano, pese a su posterior desactualización en la materia.

Consta de un título preliminar sobre disposiciones generales, un título I sobre utilización de datos personales; un título II sobre titulares de datos; un título III dedicado a la utilización de datos de carácter comercial; un título IV sobre tratamiento de datos de organismos públicos; un título V con un régimen sancionador y, finalmente, un título final con disposiciones transitorias.

En su artículo 2, señala que serán considerados como datos personales sobre los cuales se aplicará esta ley aquéllos pertenecientes a personas naturales, excluyendo así a las personas jurídicas. En cuanto a su tratamiento, éste puede ser automatizado o manual surgiendo a partir de las operaciones que se efectúen sobre los datos personales y la consiguiente creación de un banco de datos; requiriéndose, según el artículo 4 del consentimiento del titular, a menos que provengan de una fuente pública[17].

Al respecto, la fuente pública *"es uno de los conceptos más controvertidos de la ley, por cuanto basta que el titular del banco de datos defina las condiciones de no restringido o reservado para que los datos almacenados queden exceptuados de muchos de los mecanismos de resguardo que establece la ley*" (Donoso, Lorena: 2013, p. 94).

Tal como se aprecia "*La regla general formalmente declarada por el texto legal es que dicho tratamiento sólo puede hacerse en virtud de autorización legal o del titular de los datos, pero del contexto de las normas se desprende que la mayoría de los datos provienen de fuentes de acceso público – por lo cual no se requiere de autorización para su tratamiento- y se consagran importantes y amplias excepciones, lo cual transforma a la regla general en una mera declaración de principios*" (Jijena, Renato: 2013, p. 417).

En cuanto a la competencia, ésta se encuentra radicada en el tribunal civil de turno del domicilio del responsable del banco de datos de que se trate, lo que implica procedimientos extensos y costosos.

[17] El tratamiento de los datos personales solo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente a ello.
La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.
La autorización debe constar por escrito.
La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito.
No requiere autorización el tratamiento de datos personales que provengan o se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, 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 sean necesarios para comunicaciones comerciales de respuesta directa o comercialización directa de bienes o servicios.

En su catálogo de derechos, consagra los derechos de acceso, rectificación, cancelación y oposición los ya mencionados derechos ARCO y que en relación al derecho al olvido, son los dos últimos que mayormente se vinculan a éste, pero que en los términos de la Ley son los derechos que puede ejercer una persona física para controlar sus datos personales y a través de los cuales existe una mención indirecta del derecho al olvido debido a su carácter instrumental.

Estableció una acción judicial de tutela, el habeas data[18] de conformidad al artículo 16 de la Ley y que "*se configura como el instrumento a través del cual, los titulares de datos pueden ver protegidos sus derechos frente a acciones que resulten ilegales o arbitrarias o que importen un uso indebido de información de carácter personal por parte del responsable del fichero o banco de datos*" (Jervis, Paula: 2003).

En relación al régimen sancionatorio, establece multas que van de 1 a 10 unidades tributarias mensuales o de 10 a 50 unidades tributarias mensuales.

No obstante la conformación de este sistema de protección sencillo, carece de un órgano administrativo especializado que vele por el cumplimiento de la norma –como los existentes a nivel europeo y latinoamericano, siendo una de las principales deficiencias de esta ley.

Por otra parte, se aprecia en la jurisprudencia nacional que se ha prestado especial atención a una clase de datos personales determinados, aquéllos vinculados a obligaciones comerciales o bancarias y que se refleja en la creación de una norma especial, la Ley 20.575.

Sin embargo, pese a que su aplicación era delimitada a dichos datos, tampoco ha sido eficiente, puesto que no ha sido interiorizada por las empresas, debido precisamente al débil sistema general de protección de la Ley 19.628, que no es capaz de persuadir a los responsables de los datos, ya que las multas que pueden sufrir, no se comparan a las utilidades que reportan.

Lo anterior, nos muestra lo siguiente: "*aunque el tema de los datos personales va mucho más allá que el problema de los protesto, de la morosidad comercial y de los archivos históricos almacenados en el banco de datos por cierto tiempo, esta es la principal connotación que se le ha dado en Chile*" (Jijena, Renato: 2013, p. 415).

[18] "que procede en aquellos casos en que el responsable del registro o banco de datos no se pronuncia oportunamente sobre la solicitud del requirente que pide información sobre sus datos personales, modificación de los que sean erróneos, equívocos o incompletos, o eliminación de los que carezcan de sentido o estén caducos, o eliminación o bloqueo de aquellos datos proporcionados voluntariamente que no desea que continúen figurando en el registro respectivo, o cuando dicho requerimiento es denegado injustificadamente" (Banda, Alfonso: 2000, p.64).

En consecuencia, las únicas manifestaciones de derecho al olvido son aquellas contenidas en los artículos 18 de la Ley 19.628 y 10 del Decreto N° 250 de 1928 del Ministerio de Hacienda, que se refieren a la caducidad de aquellos datos personales que han permanecido en una base de datos por más de 5 años desde que la obligación se hizo exigible.

No obstante, como muestra del escueto sistema general de protección de datos no se prohíbe la perpetuidad del uso de datos caducos, por lo que en la práctica pueden seguir utilizados sin estar infringiendo la ley, dejando al ciudadano en total indefensión.

Así, conforme al análisis presentado, es posible afirmar que "*La Ley chilena, en ese sentido no cumple ese estándar puesto que no contempla el principio de control en su doble faceta: la facultad del titular de control en el tratamiento de sus datos y la existencia de un organismo público independiente que supervise la actividad de quienes tratan datos y que tenga facultades de intervención, investigación, fiscalización y sanción*"[19].

Estas preocupaciones, han influenciado la presentación de proyectos de ley que pretenden perfeccionar la legislación ya existente o directamente incluir el derecho al olvido en el ordenamiento jurídico nacional.

Así encontramos los proyectos de ley boletines 8208-07[20], 9388-03[21] y 9917-03[22] que en términos generales son mejoras al sistema de protección de datos, en base incluso al derecho al olvido, pero se advierte cuanto influye la falta de consciencia por parte de las autoridades respectivas – y también de los ciudadanos- sobre la importancia de contar con una correcta legislación sobre protección de datos personales, ya que se encuentran acotados sólo a cierto datos personales o bien no se condice con la realidad nacional.

---

[19] En VI Encuentro Ibero-Americano de protección de datos, en Cartagena de Indias, el 29 de mayo de 2008 Thomas Zerdick de la Dirección General de Justicia, Libertad y Seguridad de la Comisión europea, expuso sobre los "9 simples pasos para la adecuación".

[20] Boletín N° 8208-07 de fecha 20 de Marzo del 2012 iniciado en moción por los honorables Gonzalo Arenas, Sergio Bobadilla, Enrique Estay, Javier Hernández, Andrea Molina, entre otros. Revisado en: https://www.camara.cl/pley/pley_detalle.aspx?prmID=8608&prmBoletin=8208-07.

[21] Boletín N° 9388-03 de fecha 11 de junio del 2014 iniciado en moción por los honorables Carlos Bianchi, Francisco Chahuán, entre otros. Revisado en: https://www.camara.cl/pley/pley_detalle.aspx?prmID=9800&prmBoletin=9388-03.

[22] Boletín N° 9917-03 iniciado en moción por los honorables Felipe Harboe, Antonio Horvath, entre otros. Revisado en https://www.camara.cl/pley/pley_detalle.aspx?prmID=10337&prmBoletin=9917-03.

El primero y el segundo, pretendían obligar a las redes sociales y a los motores de búsqueda a borrar todos los datos de una persona de forma inmediata y completa si ésta así lo pide expresamente y si no existe ninguna razón de peso para retenerlos en la red. En tanto el tercero, señalaba expresamente un derecho al olvido que debe incluirse entre los derechos de titulares de datos personales, con respecto a los motores de búsqueda y sitios web en que aparezca su nombre, y para el caso de denegación, conceder una acción de habeas data.

Además, el proyecto de ley apunta a la ampliación del ámbito de aplicación del artículo 18 de la ley 19.628, estableciendo que no sólo está prohibida la comunicación de datos caducos, sino también el uso, tratamiento y transferencia de dicha información.

Por último- y no por ello menos importante- en este escenario poco fructífero en materia de protección de datos, la jurisprudencia nacional ha reflejado el principio de finalidad así como también, ha perfilado las condiciones de lo que comprende el derecho al olvido con mayor asertividad que la propia legislación, sin embargo, lo vincula a otros derechos fundamentales y no con el derecho a la protección de datos personales como tal.

Así, en Sentencia dictada por la Corte Suprema Causa Rol N° 1705/2012 de 24 de Septiembre del año 2012; sobre recurso de protección referido a la mantención en registro de datos de información crediticia de una persona física sin justificación legal[23], se pronunció favorablemente para la parte demandante de conformidad a la Ley y al derecho a la honra y señaló que:

> *(10)" es evidente que el banco acreedor o sus cesionarios no han demostrado al menos por un periodo de cinco años voluntad en recuperar su acreencia y, en segundo término, porque en esas condiciones y al tenor del artículo 6 de la Ley Nº 19.628 el dato en cuestión adquirió al menos la categoría de dudoso a la luz de esa disposición, teniendo en consideración que dicho lapso de tiempo supera el previsto por la legislación procesal para exigir que se declare el abandono del procedimiento y excede también el que requiere el derecho sustantivo para obtener*

[23] Doña Rosa Hidalgo Aguirre ha deducido acción de protección de derechos constitucionales en contra del Banco BBVA, por cuanto figura en un registro informal y clandestino que fue deudora con dicha institución en el año 2003, todo lo cual conoció al rechazársele una solicitud para un crédito hipotecario en el Banco Itaú, pese a que no tiene antecedentes en Dicom ni en la Superintendencia de Bancos e Instituciones Financieras.

la declaración de prescripción de las obligaciones. A este respecto, el artículo 9 de la referida ley dispone: "En todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos"

(12) "Que las conductas descritas conculcan el derecho constitucional de la recurrente previsto en el artículo 19 numeral 4º de la Constitución Política de la República, al afectar su honra, toda vez que es evidente que la inclusión de una deuda en un registro de morosidades desacredita la fama de una persona cuando le imposibilita la obtención de un crédito por considerarla insolvente, cuando en realidad no lo es.

Un importante ejercicio jurisprudencial, es la Sentencia 228/2012 de la Corte de Apelaciones de Valparaíso de 30 de Julio que en relación a un recurso de protección presentado por injurias en sitios web [24] concedió lo solicitado, en razón del derecho a la vida privada y al honor establecidos en el artículo 19 N°4, pero además señaló acciones concretas que asegurarían el completo resarcimiento del ciudadano y que constituyen reconocimiento tácito al derecho al olvido.

En efecto, en su considerando tercero la Corte advirtió:

"Que, no obstante haberse informado que alguna de las publicaciones infamantes, han sido eliminadas de determinadas páginas web (…) existe una persistencia en la publicación de los referidos contenidos".

Y por lo mismo en su considerando cuarto estableció que no sólo procede la eliminación de la información injuriosa sino:

"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 como la de autos"

[24] El abogado, Jorge Abbott presentó dicho recurso en contra de los administradores de una serie de sitios web, puesto que en ellos se difundía información falsa que comprometía tanto a él como a su familia, fundado en el artículo 19N°4 de la CPR , solicitando por consiguiente la eliminación de toda dicha información injuriosa.

IV. Conclusiones

Es momento de hacernos cargo de una crítica que deslizamos al comienzo de este texto, esto es la falta de una definición. Para ello tomamos distintos elementos contenidos en el desarrollo del análisis, según lo cual podemos decir que el derecho al olvido es un mecanismo jurídico que se manifiesta en la facultad que tiene toda persona natural, de solicitar a la autoridad competente, que ordene la eliminación y/o desindexación de datos o información, de carácter personal, al responsable de su tratamiento, por haber una falta de consentimiento o un retracto en el consentimiento entregado por el titular del derecho, cuando ya se hayan cumplido los fines para los que fueron recopilados, cuando los datos fueren inexactos, falaces o desactualizados o cuando no se hayan resguardado diligentemente los datos almacenados.

Consideramos que es el concepto más idóneo y que contiene todos los elementos necesarios para una efectiva tutela de la protección de datos.

Es necesario decir que los principios de la protección de datos –consentimiento, finalidad, calidad y seguridad- son los mismos que se aplican al derecho al olvido.

Como ya se señaló en su oportunidad, ambos temas están íntimamente relacionados pues si no existe una normativa contundente sobre protección de datos de nada sirve establecer el derecho al olvido como mecanismo jurídico. Sería como si existiese un recurso de protección, pero no se establezcan los derechos que cautela o simplemente no existan derechos que resguardar.

Como propusimos en el concepto anteriormente analizado, el derecho al olvido procedería ante una infracción a los principios que se encuentran consagrados en la norma de protección de datos, principios que comparten tanto la Directiva de la comunidad europea, la ley española de protección de datos y la ley chilena sobre protección de la vida privada.

Antes de que los Estados comenzaran a crear normativa relativa a la protección de datos en específico, el mecanismo para protegerlos era mediante una vulneración de otros derechos como la vida privada, la intimidad o la honra. A esto le llamamos una protección indirecta,

pues no protege los datos en cuento bien jurídico en sí mismos, sino que solo en cuanto el tratamiento de estos vulnera otro derecho como los anteriormente dichos.

En nuestro país, eso es lo que ocurre ya que no tenemos una consagración constitucional sobre protección de datos, por tanto, si se quiere reclamar por el tratamiento de sus datos, debe demostrar que el tratamiento de sus datos vulneró un derecho como la vida privada, la intimidad o la honra.

Por el contrario, en España y en los países de la comunidad europea se protegen los datos en cuanto tales y no se requiere que el tratamiento de estos haya vulnerado otro derecho, pues la protección de datos es un derecho en sí mismo.

En referencia al derecho comparado, el permanente debate y desarrollo normativo en materia de protección de datos en Europa, da cuenta de una cultura jurídica tanto a nivel comunitario e interno que proviene desde sus orígenes en el Convenio 108 pasando por la Directiva 95/46/CE y que ha alcanzó su mayor expresión en la Sentencia del Tribunal de Justicia Europeo contra Google; en que se reconoció un derecho al olvido, y en el Proyecto de Reglamento de Protección de Datos que lo consagra de manera expresa.

De modo similar, Latinoamérica en los últimos años ha obtenido importantes avances en materia de protección de datos como México, que ha creado su órgano garante independiente e incluso inició una controversia jurídica contra Google México; Argentina y Uruguay, siendo este último un modelo ejemplar pues cuenta con un sistema de protección de datos propio; estableciendo plazos de caducidad para el tratamiento y difusión de la información, un derecho de los datos personales autónomo a los cuales clásicamente estaba asociado, es decir, a la honra y la vida privada, por lo que ha alcanzado la categoría de países con condiciones adecuadas de acuerdo a los criterios europeos.

En cuanto al Proyecto de Reglamento del Consejo Europeo en materia de protección de datos, este posee un valor innegable como primer instrumento jurídico vinculante a nivel comunitario, otorga al consentimiento el carácter de presupuesto central para el tratamiento de los datos personales, y además efectúa el más importante aporte al señalar como responsable del tratamiento a los recopiladores originales de la información personal. Sin embargo lo anterior también resulta ser un punto débil, pues deja de lado al motor de búsqueda, en

circunstancias que la Sentencia de Costeja VS Google Inc. contó con un razonamiento jurídico que giró en torno a que el motor de búsqueda también es responsable al momento de cancelar los datos personales; ya que no obstante eliminarse la información por parte del que recopiló, esta seguía apareciendo en los índices de resultados de búsqueda.

Con todo, debiese tratarse de una responsabilidad compartida, por una parte del recopilador original, su sitio web y por otra, el motor de búsqueda como herramienta de localización de resultados, cuestión que esperamos sea modificada a través de las enmiendas del Consejo Europeo, ya que pese a que fue aprobado en general aún se encuentra en discusión.

En el caso de Chile la Ley 19.628 sobre protección a la vida privada, no cuenta siquiera con un nivel mínimo de protección de datos personales, por ende se carece de un marco jurídico previo que sea idóneo, para que nuestro país integre y desarrolle un derecho al olvido.

Su tenor evidencia que se ha construido sobre las base del derecho a la vida privada, desconociendo y no reflejando que lo primordial en materia de protección de datos, son estos mismos; de modo que el control de su tratamiento se fundamenta en consideraciones que van más allá del derecho a la vida privada, a la honra, entre otros.

La insuficiencia y debilidad de esta Ley se aprecia en el plano institucional, ya que a diferencia de la situación de países europeos o incluso también latinoamericanos, Chile es prácticamente el único país que carece de un órgano que fiscalice el cumplimiento de la ley y al cual poder recurrir frente a la vulneración de sus derechos, siendo materia de competencia de la justicia civil ordinaria, con un régimen sancionatorio con multas menores y que sólo acarrea responsabilidad en sede civil. Asimismo, los denominados derechos ARCO, no pasan de ser meramente declarativos, pues están regulados a modo superficial y establecen limitaciones que se refieren a conceptos amplios

Pese a que el poder legislativo ha demostrado preocupación al respecto, como lo demuestra los proyectos de ley que se han presentado- algunos con mayor fortuna de razonamiento que otros - no identifican correctamente este problema; toda vez que sus propuestas resultan ser insuficientes, pues se sustentan en la actual legislación- insuficiente y débil como ya advertimos- y más grave aún no se hacen cargo de la labor de protección previa que debe existir en protección de datos en cuanto tales.

Por otra parte, no obstante que la jurisprudencia nacional analizada fue favorable para el recurrente, la realidad es que un sin número de recursos no son acogidos, de modo que se carece de criterios jurídicos uniformes arraigados en los operadores jurídicos.

En consecuencia, frente a la interrogante de si el derecho al olvido tiene cabida y de ser afirmativa la respuesta, el cómo debería integrarse este mecanismo a nuestro ordenamiento jurídico. Cabe señalar que no, pues conforme al análisis practicado; primero debe existir un reconocimiento constitucional del derecho a la protección de datos, que permita generar una cultura en materia de protección de datos tanto en el ámbito intelectual como el del ciudadano común- siendo incluso más importante éste último- ya que son quienes deben comprender y dimensionar que cuentan con una protección para sus datos personales por sí mismos, pudiendo llevar un control del tratamiento que se les confiere y que por lo mismo, frente a una agresión o vulneración a estos deben iniciar los procedimientos pertinentes.

Así , cumplida idealmente la fase anterior se debe proceder lisa y llanamente a nueva ley en materia de datos personales que permita que un mecanismo jurídico como el derecho al olvido sea efectivo y no una mera declaración; que cree un órgano desconcentrado y especializado en la materia, para entregar información y al cual dirigirse en caso de afectación.

Por tanto, para la procedencia del derecho al olvido en Chile se requiere de una simultaneidad de elementos que confieran un marco jurídico suficiente para su establecimiento y efectividad, a saber: datos personales como derecho fundamental; cultura en materia de protección de datos, desarrollo de una institucionalidad propia; vía administrativa; sanciones persuasivas y derechos arcos, en éste orden.

V. Referencias bibliográficas

Papers.

1. Abril, Patricia y Pizarro Eugenio (2014): "La intimidad europea frente a la privacidad americana", en Revista para el análisis del derecho, Barcelona, N° 1, pp.1-62. Disponible en: http://derechoaleer.org/media/files/olvido/1031.pdf. Fecha última consulta: 15/10/2015.

2. Bru, Elisenda (2007) "La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad" en Revista de los Estudios de Derecho y Ciencia Política de la. ISSN 1699-8154, Nº 5.

3. Cerda, Alberto. (2003) "Autodeterminación informativa y leyes sobre protección de datos". Disponible en: http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/view/10661/11413 . Fecha última consulta: 14/10/2015.

4. Cortés, Carlos (2012): "Derecho al olvido: entre la protección de datos, la memoria y la vida personal en la era digital", en CELE. Centro de Estudios en Libertad de Expresión y Acceso a la Información, Buenos Aires. Disponible en: http://carloscortes.co/mi-trabajo/2013/8/27/derecho-al-olvido-entre-la-proteccin-de-datos-la-memoria-y-la-vida-personal-en-la-era-digital . Fecha última consulta: 14/10/2015.

5. Delpech, H. (2015). Derecho al Olvido en Internet. Obtenido de XIX Congreso Iberoamericano de Derecho e Informática: http://fiadi.org/mesa-1-proteccion-de-datos-personales/. Fecha última consulta: 15/10/2015.

6. Donoso, Lorena (2013) "Derechos Humanos y Derechos Fundamentales en la Sociedad de Red", en Ciudadanas 2020. II El. Gobierno de la Información. LOM, Santiago de Chile, pp. 78-109.

7. Gallardo, Marc (2012) "El Derecho al Olvido digital en la Unión Europea" en http://www.uianet.org/sites/default/files/27.02.13.Olvido.UIA(1).pdf Fecha última consulta 23/09/2015.

8. Garrido, Romina (2013) "El Habeas Data y la Ley de Protección en Chile "en Serie Bibliotecología y Gestión en la Información N°83, junio.UTEM. Revisado en: http://eprints.rclis.org/19755/1/Serie%20N%C2%B0%2083%2C%20Junio%2C%202013%20Actualizada.pdf Fecha última consulta: 08/11/2015.

9. Hernández, Mario (2013): "El derecho al olvido digital en la red 2.0", en Cuaderno Red de Cátedras Telefónica, N° 11 de mayo de 2013. Disponible en: http://catedraseguridad.usal.es/sites/default/files/files/CUADERNO_11_DERECHO%20OLVIDO.pdf. Fecha última consulta 15/10/2015.

10. Jervis, Paula. Derechos del Titular de Datos y Habeas data en la Ley 19.628. Revista Chilena de Derecho Informático, n. 2, ene. 2003. ISSN 0717-9162. Disponible en: http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/view/10644/11372 .Fecha última consulta: 11/11/2015.

11. Jijena, Renato (2010) "Actualidad de la Protección de Datos Personales en América Latina. El Caso de Chile" XIV Congreso Iberoamericano de Derecho e Informática de la Universidad Autónoma de Nuevo León, "Revolución Informática con Independencia del Individuo"

12. Reyes, Patricia (2015). "Regulación de la Protección de Datos Personales en Chile: Deficiencias y Desafíos". Publicación pendiente. (texto proporcionado por el autor) Chile.

13. Simón, Pedro (2012) "El derecho al olvido en el universo 2.O", BiD: textos universitaris de biblioteconomia i documentació, núm. 28. http://bid.ub.edu/28/simon2.htm Fecha última consulta: 24/09/2015.

14. Tabernero, Silvia (2014): "El derecho al olvido", en Trabajo de fin de grado, Universidad de Salamanca. Disponible en http://gredos.usal.es/jspui/bitstream/10366/123843/1/TFG%20_TaberneroMartin_Derecho.pdf. Fecha última consulta: 01/08/2015.

15. Terwangne, Cécile de (2012): "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido", en VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet. Revista de Internet, Derecho y Política. N. º 13, pág. 53-66. Disponible en http://idp.uoc.edu/index.php/idp/article/view/n13-terwangne_esp/n13-%20terwangne_esp . Fecha última consulta: 11/05/2015.

16. Troncoso, Antonio (2012): El derecho al olvido en Internet a la luz de la propuesta de reglamento general de protección de datos personales de la Unión Europea en Revista de Derecho, Comunicaciones y Nuevas Tecnologías, N° 8 Diciembre, pp. 2-38. Disponible en http://dialnet.unirioja.es/servlet/articulo?codigo=4053425. Fecha última consulta: 14/10/2015.

17. Troncoso, Antonio (2010): "La protección de datos personales. En busca del equilibro", Tirant lo Blanch, Valencia: 2010, pp. 816-831

Legislación

18. Decreto N° 250 de 1928 sobre boletines comerciales. Disponible en http://www.leychile.cl/Navegar?idNorma=254568&r=1. Fecha última consulta: 05/12/2015.

19. Ley 19.628 sobre protección de la vida privada. Disponible en http://www.leychile.cl/N?i=141599&f=2012-02-17&p=1. Fecha última consulta: 20/07/2015.

20. Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal. Disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/index-ides-idphp.php Fecha última consulta: 20/07/2015.

21. Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 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. Disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/index-ides-idphp.php Fecha última consulta: 20/07/2015.

22. Propuesta de Reglamento de protección de datos http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/es/pdf Fecha última consulta: 14/10/2015.

23. Comunicación Parlamento Europeo de Bruselas 2010 Disponible en http://ec.europa.eu/health/data_collection/docs/com_2010_0609_es.pdf Fecha ultima consulta: 14/10/2015.

24. Convenio 108 disponible en http://www.coe.int/t/dghl/standardsetting/DataProtection/Global_standard/D%C3%A9pliant%20Conv108_es.pdf Fecha última consulta: 15/10/2015.

Jurisprudencia

25. Sentencia de Dirección Nacional de Protección de Datos Personales, Argentina, de 19 de Noviembre de 1999 en http://www.infojus.gob.ar.

26. Sentencia Corte de Apelaciones de Valparaíso, "Jorge Abbott Charme c/ Google", Rol Nº 228-2012, de 30 de julio de 2012. En www.poderjudicial.cl Fecha última consulta: 20/09/2015.

27. Sentencia Corte Suprema, "Banco BHIF/Hidalgo Aguirre Rosa", Rol 1705/2012. En http://iura.cl/jp/suprema/2012/1705.html Fecha última consulta 28/10/2015.

28. Sentencia Tribunal Supremo de Justicia Europea de 13 de Mayo de 2014 disponible en http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES. Fecha última consulta 24/10/2015

Sitios web

29. Derecho Chile (26 de Junio de 2014) http://www.derecho-chile.cl/proteccion-de-datos-personales-parte. Fecha última consulta: 4 de octubre de 2015.

30. Derecho Chile (8 de Julio de 2014) http://www.derecho-chile.cl/proteccion-de-datos-personales-ii-parte. Fecha última consulta: 4 de octubre de 2015.

31. Concepto definición (n.a.) http://conceptodefinicion.de/indexacion. Fecha última consulta: 7 de octubre de 2015.