UNIVERSIDAD DE CHILE

FACULTAD DE DERECHO

DEPARTAMENTO DE DERECHO PROCESAL

LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS DESCRIPCIÓN Y ANÁLISIS DE SU ROL EN LA PROTECCIÓN A LA VIDA PRIVADA Y TRATAMIENTO DE DATOS PERSONALES EN LAS REDES SOCIALES

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

PALOMA JESÚS HERRERA CARPINTERO

Profesor guía: Daniel Álvarez Valenzuela

Santiago, Chile

2016

TABLA DE CONTENIDO

RESUMEN.

El objeto de esta memoria consiste en describir y analizar el importante rol de la Agencia Española de Protección de Datos, como autoridad de control autónoma e independiente, encargada de velar por el cumplimiento del derecho a la intimidad y derecho a la protección de datos personales en el ámbito de las redes sociales. El uso de estas plataformas virtuales conlleva a que las personas sobrexpongan su vida privada a través del contenido que comparten en ellas, generando el peligro de que terceros mal intencionados utilicen con fines ilícitos dicha información. Así, a consecuencia de los diversos conflictos que surgen con el uso de las redes sociales, la Agencia Española de Protección de Datos ha sido la entidad encargada de fiscalizar y sancionar a los responsables por tratamiento indebido de datos, otorgando en consecuencia eficiencia y eficacia a la normativa de protección de datos vigente en España. Mientras que en Chile nuestra actual normativa y la reforma en tramitación no contemplan la existencia de una autoridad con estas características, quedando en consecuencia el ciudadano desprotegido frente al tratamiento indebido de sus datos en las redes sociales y en el ámbito de las tecnologías en general.

INTRODUCCIÓN.

Con el avance de la tecnología y, en específico, el progreso de internet, la forma en que se desenvuelve y relaciona la sociedad está en constante evolución. Así, uno de los grandes hitos en esta era de la información y las telecomunicaciones es el auge de las redes sociales. Sin embargo, el uso de estos espacios *online* no está exento de preocupaciones, pues los riesgos generados contra la privacidad y datos personales de sus usuarios y terceros son innumerables.

Las personas, en general, son inconscientes y muchas veces ignoran las consecuencias que conlleva el compartir su privacidad y datos personales en internet, lo cual facilita que terceros mal intencionados utilicen dicha información con fines ilícitos. Por otro lado, los principales proveedores de servicios de redes sociales establecen condiciones de uso abusivas descuidando la privacidad de sus usuarios. Ambas consideraciones tienen como resultado que la transgresión al derecho de privacidad, desde su perspectiva informacional, haya aumentado exponencialmente en el último tiempo.

Como consecuencia de la situación anteriormente descrita, es necesario que la legislación vigente en materia de privacidad y protección de datos personales pueda ser aplicada en el nuevo escenario que plantean las redes sociales. Para estos efectos, no basta con que el ordenamiento jurídico reconozca la existencia de diversos mecanismos fiscalizadores y sancionadores si estos no se pueden aplicar de forma efectiva en un caso en concreto. En efecto, las principales problemáticas que conlleva la aplicación de la normativa existente en protección de datos personales en el ámbito de las redes sociales, son las siguientes:

- La dificultad de esclarecer el paradigma de lo público y lo privado.
- La expectativa de privacidad del usuario de las redes sociales.
- La dificultad de ejercer la potestad de fiscalización y coerción ante los responsables de tratamiento de datos, ubicados fuera del territorio nacional. Como ocurre con los proveedores de servicios de redes sociales, algunos usuarios y desarrolladores de aplicaciones.

En España, gracias a la labor realizada por la Agencia Española de Protección de Datos (en adelante, "Agencia" o "AEPD", indistintamente),

han logrado aplicar de forma efectiva la normativa vigente en el ámbito de las redes sociales por las razones que se exponen a continuación:

- Han educado al usuario respecto a los peligros contra la privacidad que conlleva el uso de las redes sociales, así como han otorgado mecanismos administrativos de fácil acceso para que estos puedan ejercer sus reclamaciones frente a la vulneración de sus derechos.
- Al ser un organismo técnico y especializado en materia de privacidad y protección de datos personales, ha podido generar diversos criterios de interpretación de la legislación vigente con la finalidad de adecuar su utilización en el ámbito de las redes sociales.

Ciertamente lo anterior dista mucho de la realidad jurídica vivida en Chile, toda vez que nuestro país ha sido catalogado en múltiples ocasiones como un país que no cumple con un estándar adecuado de privacidad, como consecuencia de tener una legislación obsoleta en materia de protección de datos. Apropósito de esto, destaca como principal crítica la carencia de una autoridad de control, independiente y especializada en protección de datos, que se encargue de dar eficacia y eficiencia a la normativa contenida en ella. De lo anterior resulta lo siguiente:

- Al carecer de una entidad que ejerza las potestades de coerción y sanción en materia de protección de datos personales, el único mecanismo de reclamación existente en Chile es en sede judicial. Por tanto, al analizar las personas el costo-beneficio de recurrir a la judicatura en aquellos casos que involucren el uso de las redes sociales, deciden no perseverar en el asunto.
- La actual normativa no reconoce facultades de oficio, lo que sumado a la inexistencia de una autoridad de control, produce que no se puedan inspeccionar e investigar de forma efectiva aquellos conflictos que involucren el uso de estas plataformas.
- Falta de difusión e información respecto a los peligros que conlleva el uso de las redes sociales, y los derechos que tienen los ciudadanos relativos a esta materia.
- Falta de informes y desarrollo de criterios, por parte de la doctrina y jurisprudencia, respecto a la adecuación de la normativa vigente en el ámbito de las redes sociales.

Es en razón de estas consideraciones que he de describir y analizar la experiencia española, a través de su Agencia Española de Protección de Datos, con la finalidad de demostrar lo trascendental de su rol en el

resguardo de la privacidad y los datos personales, así como también recalcar la imperiosa necesidad de contar con una entidad con dichas características en nuestro país.

De esta forma, en el primer capítulo haré referencia al derecho a la vida privada, sus orígenes, la evolución que este ha experimentado en el tiempo y su desarrollo tanto doctrinal como normativo. Desde este punto, haré mención a la perspectiva informacional de este derecho, materializada en el derecho a la protección de datos personales, refiriéndome a sus alcances, principios y objetivos.

En el segundo capítulo describiré el marco jurídico general de la privacidad y protección de datos personales a la luz del derecho chileno. Desde esta perspectiva, realizaré un análisis crítico la Ley 19.628 "Sobre protección de la vida privada y protección de datos de carácter personal" y el actual anteproyecto de ley que introduce modificaciones en esta materia. Para tales efectos, destacaré como principal falencia la ausencia de consagración de una autoridad de control que tenga por afán cumplir de forma efectiva esta normativa.

En el capítulo tres describiré, desde la arista española, la Ley Orgánica 1/1982 de "Protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen", la Ley Orgánica 15/1999 de "Protección de datos de carácter personal", el Real Decreto 1720/2007 que aprueba el Reglamento de desarrollo de la Ley Orgánica de protección de datos con énfasis en la normativa comunitaria de la Unión Europea, destacando la Directiva 95/46/CE. Lo anterior nos permitirá interiorizarnos en la comprensión del derecho español, lo que posibilitará el entendimiento del cuarto capítulo, en el cual describiré la Agencia Española de Protección de Datos, abarcando tanto su estructura así como naturaleza jurídica y principales funciones, con énfasis en el elemento de independencia que detenta dicha entidad.

En el capítulo quinto me centraré en la evolución que ha experimentado la internet hasta llegar al actual auge de las redes sociales, estudiando su definición, clasificación y diversos tipos. Haré una relación detallada de las principales amenazas a la privacidad y protección de datos que se plantean en las redes sociales. En cada situación señalaré cómo se afectó el derecho a la intimidad y/o protección de datos personales, señalando ejemplos

mediáticos en los cuales se vulneró este derecho a través de la utilización de Facebook y Twitter.

Para finalizar, en el capítulo seis se analizan los principales requerimientos y resoluciones emanados de la Agencia Española de Protección de datos en materia de redes sociales entre los años 2010 a 2015. De tal forma, circunscribiré el estudio al procedimiento de tutela de derechos y procedimiento sancionador, permitiendo de esta forma entender los principales criterios construidos por la Agencia a fin de adecuar la normativa imperante en el ámbito de las redes sociales y, de esta forma, asegurar la eficiencia y eficacia del sistema normativo español en el ciberespacio.

I. ASPECTOS GENERALES DEL DERECHO A LA VIDA PRIVADA Y PROTECCIÓN DE DATOS PERSONALES.

Desde tiempos inmemoriales el hombre comprendió la trascendencia de proteger su privacidad y de mantener ciertas áreas de su vida ajenas a la intromisión de terceros, pues solo de esta forma los individuos pueden desarrollar libremente su personalidad. Sin embargo, a lo largo del tiempo, este derecho ha sufrido múltiples cambios debido al surgimiento de nuevas amenazas que atentan contra la privacidad.

El desarrollo de las nuevas tecnologías de la información y comunicación (en adelante, "TIC", indistintamente), es en la actualidad una de las principales preocupaciones de los diversos ordenamientos jurídicos. En efecto, si bien otorgan grandes beneficios a la sociedad desde el punto de vista de la eficiencia y la interconectividad, traen aparejadas diversas amenazas tendientes a vulnerar la vida privada de los sujetos por intermedio de estos instrumentos tecnológicos. Así, el riesgo se presenta, ya sea mediante la recopilación y tratamiento de datos personales de forma arbitraria e ilegal o en el ejercicio de la libertad informática, la que colisiona

en muchas ocasiones con el derecho de un individuo al secreto de su vida privada[1].

En razón de lo anterior, todo Estado que se considere democrático tiene la obligación de reforzar los distintos mecanismos de protección a la intimidad, y, por ende, al derecho a la protección de datos personales. Para tales efectos, es imperioso comprender los límites actuales de la privacidad e identificar las diversas situaciones que quedan bajo su amparo. Por tal motivo, analizaré en este capítulo el desarrollo histórico y conceptual del derecho a la vida privada y la protección de datos personales con el objeto de obtener una visión teórica general, la cual es fundamental para poder entender en los siguientes apartados la crítica que hago a la realidad chilena a la luz de la descripción y análisis de la experiencia española respecto a esta materia.

[1] NOVOA M., Eduardo. 1979. Derecho a la vida privada y libertad de información. México, Siglo XXI Editores. pp. 9-12.

1. Derecho a la vida privada.

1.1. Origen histórico y fundamento.

Los primeros atisbos de la noción de intimidad estaban arraigados a un punto de vista territorial basado en la propiedad privada. El derecho a la vida privada se proyectaba en el deseo de un pequeño y selecto grupo de proteger su hogar e intimidad. Como señala el profesor Carlos Peña, "en el Medioevo, la intimidad aparece solo en aquellas personas que pertenecen a la nobleza o ligadas al clero, situación privilegiada que les permitía apartarse o aislarse de la sociedad"[2]. En efecto, la propiedad privada era considerada como requisito esencial para ser titular del derecho a la intimidad.

Es a finales del siglo XVIII, en pleno desarrollo de la Revolución Industrial, donde la noción de intimidad adquiere relevancia, al extender el reconocimiento de este derecho a un mayor número de personas debido al surgimiento de una nueva clase social: la burguesía[3]. A partir de este punto,

[2] PEÑA G., Carlos. 1996. El Derecho Civil en su relación con el Derecho Internacional de los Derechos Humanos. En: Sistema jurídico y derechos humanos: el derecho nacional y las obligaciones internacionales de Chile en materia de Derechos humanos. Santiago, Universidad Diego Portales. pp. 561.
[3] Ibíd. p.561.

la privacidad comienza a ser concebida como el derecho que tiene todo hombre a repeler la intromisión de terceros en su morada, su santuario.

Más adelante, durante el siglo XIX, la privacidad adquiere relevancia como valor digno de tutela jurídica, al ser considerada una proyección de la libertad individual que tienen todos los hombres. El derecho a la vida privada se concreta en la libertad que tiene toda persona a negar el acceso o conocimiento a aquello perteneciente a lo más profundo de su ser, sin que el Estado soberano o la sociedad intervengan en las conductas privadas de cada individuo, teniendo como único límite la no afectación de los intereses de los demás[4].

Como podemos observar, el ideario de intimidad se ha desplegado desde tiempos remotos, sin perjuicio de que ha ido variando su contenido en el transcurso de las épocas, producto de la evolución natural de toda sociedad. Sin embargo, el reconocimiento del derecho a la vida privada como institución jurídica autónoma, desligada por completo de otros derechos, como lo son el de propiedad o libertad, es una construcción de tiempos recientes.

[4] CORRAL T., Hernán. 2000. Configuración jurídica del derecho a la privacidad I: Origen, desarrollo y fundamentos. Chile, Revista Chilena de Derecho. 27(1). 53-54pp.

La consolidación de la intimidad como derecho tiene su origen en el artículo *The right of privacy*[5] elaborado por los abogados norteamericanos Samuel Warren y Louis Brandeis en el año 1890. El ensayo aborda la problemática de los medios de comunicación y sus intromisiones en la vida privada de las personas[6]. Al respecto los autores señalan:

> "La intensidad y complejidad de la vida, atendido los avances de la civilización, han hecho necesario un cierto apartamiento del mundo, y el hombre, bajo el refinado influjo de la civilización, ha llegado a ser más sensible a la publicidad; de modo que la soledad y la privacidad han llegado a ser más esenciales para el individuo. Pero las empresas e inventos modernos, invadiendo su privacidad le han producido un sufrimiento mental y angustia mayor que la que se le podría infligir por una mera lesión corporal"[7].

[5] WARREN, Samuel y BRANDEIS, Louis. 1890. The Right to Privacy. Estados Unidos, Harvard Law Review. 4(5)

[6] Samuel Warren estaba casado con la hija de un conocido senador de Estados Unidos. Por este motivo, su esposa siempre estuvo bajo el escrutinio de la prensa local respecto a facetas que corresponderían a su vida privada y a la de su familia. Lo anterior motivó a Warren a escribir junto a Brandeis el artículo en comento en un intento de frenar la actividad sensacionalista de algunos periódicos de Boston.

[7] WARREN, Samuel. y BRANDEIS, Louis. 1890. The Right. p. 196. Citado en CORRAL T., Hernán. Configuración, Óp. Cit. p. 54.

La propuesta de esta publicación consiste en establecer los límites jurídicos de la privacidad mediante el reconocimiento de la *privacy* como derecho autónomo derivado del principio de la inviolabilidad de la personalidad. Los autores en comento cimentaron la idea de este nuevo derecho en la célebre frase acuñada, con anterioridad, por el juez norteamericano Thomas Cooley: "*The right to bet alone*"[8]. Si bien el juez Cooley utilizaba dicha locución para definir el derecho individual de toda persona a repeler las intromisiones a su domicilio y documentos privado por parte del gobierno y público en general[9], Warren y Brandeis otorgaron un significado nuevo a dicha frase, al definir *privacy* como "el derecho del individuo a determinar, ordinariamente, en qué medida sus pensamientos, sentimientos y emociones deben ser comunicados a otros"[10].

Es importante señalar que dicha definición es otorgada no solo desde una perspectiva negativa, sino que también es reconocida en ella la faceta dinámica de este derecho. De esta forma, por un lado, otorga la facultad de

[8] COOLEY, Thomas. 1879. A Treatise on the Law of Torts, Or the Wrong which Arise Independently of Contract. Callaghan, Chicago. 29p.
[9] SALDAÑA, María. 2012. The right to privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: El centenario legado de Warren y Brandeis. Revista de Derecho Político (85):196-239.
[10] WARREN, Samuel. y BRANDEIS, Louis. The Right, óp. cit. p.198. Traducción propia.

excluir a terceros de ciertos conocimientos considerados privados, concediendo el derecho a ser dejado en paz en este ámbito y, por otro, otorga un poder de control sobre el caudal de información que se manejan referida a hechos o datos de su persona[11].

Warren y Brandeis reconocieron el peligro latente que suponían las nuevas tecnologías contra la privacidad de las personas, siendo cautos en no describir de forma restrictiva los posibles medios tecnológicos que pudiesen violar la *privacy*, dando lugar a una interpretación flexible y perdurable hasta nuestros días, frente a las nuevas amenazas tecnológicas que van surgiendo con el paso del tiempo.

Con posterioridad a este hito, el concepto de privacidad y su declaración como derecho comienzan a tener un reconocimiento progresivo en los diversos ordenamientos jurídicos del mundo, llegando a alcanzar la categoría de derecho fundamental.

En este contexto, parece certera la opinión del jurista italiano Stefano Rodotà, quien afirma que la noción de vida privada, en virtud de sus peculiares características, más que un derecho debiese ser considerado un

[11] BANDA, Alfonso. 2000. Manejo de datos personales. Un límite al derecho a la vida privada. Revista de Derecho Valdivia 11: 55-70.

principio. Solo de esta forma "no sería susceptible de una interpretación literal y rígida que impida la posibilidad de intervenir sobre nuevas manifestaciones del derecho impensables en el momento de la promulgación de la norma constitucional"[12]. Como he afirmado, el concepto y los límites de la vida privada mutan con el pasar de los años, como resultado de los nuevos peligros que surgen para la esfera privada de los individuos. Así las cosas, la evolución social es un umbral vertiginoso en el cual el legislador se queda en el pasado.

En este contexto, es indispensable referirse al fundamento del derecho a la vida privada, ya que solo de esta forma podremos entender lo trascendental de la privacidad y su imperiosa necesidad de protección.

La noción de dignidad adquiere importancia en tiempos modernos, al ser considerada el fundamento de los derechos humanos y, en consecuencia, también, del derecho a la vida privada, al ser este parte integrante de estos derechos. Si bien, en épocas anteriores encontramos antecedentes respecto a

[12] RODOTA, Stefano.1973.Elaboratori elettronici e controllo sociale, Il Mulino. Citado en: PEREZ L., Antonio. 2012. Los derechos humanos en la sociedad tecnológica. España, Editorial Universitas. 325p.

la importancia de la dignidad del hombre como fuente de ciertos derechos[13], se atribuye a las devastadoras consecuencias de la Segunda Guerra Mundial el reconocimiento explícito y jurídico de la dignidad como fuente generadora de los derechos humanos, y como corolario, del derecho a la privacidad. Las aberrantes vulneraciones sufridas por la humanidad en la guerra y la toma de conciencia, por parte de la sociedad, de los peligros que involucran los adelantos tecnológicos y medios de comunicación, tienen como consecuencia el reconocimiento sistemático de la dignidad como fundamento de los derechos del hombre.

Para entender la noción de dignidad, es pertinente la definición otorgada por el catedrático español Jesús González:

> "La dignidad humana es una cualidad intrínseca, irrenunciable e inalienable de todo y a cualquier ser humano, constituyendo un elemento que cualifica al individuo en cuanto tal, siendo una cualidad integrante e irrenunciable de la condición humana. Ella es asegurada, respetada, garantizada y promovida por el orden jurídico estatal e

[13] En las polis griegas los únicos que tenían ciertos beneficios, emanados de su dignidad, eran los ciudadanos. En la Edad Media, la dignidad era vinculada a la fe cristiana. Sin embargo, en ninguno de estos momentos históricos se reconoció explícita y jurídicamente la dignidad como fuente de derecho. Cfr. NOVOA M., Eduardo. Derecho a la vida privada y Libertad de Información. Óp. Cit.13p.

internacional, sin que pueda ser retirada a alguna persona por el ordenamiento jurídico, siendo inherente a su naturaleza humana; ella no desaparece por más baja y vil que sea la persona en su conducta y sus actos"[14].

En síntesis, la dignidad se considera un elemento de la esencia vinculado a la condición humana y, por ende, corresponde a todos por igual. Asimismo, dota a todo individuo de la capacidad de autodeterminación consciente y responsable de su vida, exigiendo el respeto de ella por los demás.[15] Adelantándonos en la materia, es en virtud de estas características fundamentales de la noción de dignidad que podemos entender el concepto esencial de privacidad desde la perspectiva de autodeterminación. De este modo, el derecho a la vida privada concede la facultad a todo individuo de ejercer control sobre aspectos de su vida considerados privados, exigiendo respeto por parte de la sociedad. Lo anterior será profundizado en la segunda parte del presente capítulo.

[14] GONZÁLEZ, Jesús. 1986. La dignidad de la persona. Madrid, Editorial Civitas. Citado en: NOGUEIRA, Humberto. 2010. Dignidad de la persona, derechos fundamentales y bloque constitucional de derechos: una aproximación desde Chile y América Latina. Revista de Derecho (5):79-142.
[15] Ibíd. 2p.

La noción de dignidad no debe ser concebida desde un punto de vista individual. Es en la interacción social donde se vislumbra el sentido de dignidad y, en consecuencia, de la privacidad. Lo privado tiene existencia en la medida que está en pugna con lo público. Ante la amenaza del escrutinio por parte de la sociedad es que el hombre recela ciertos ámbitos de su vida. Es en virtud de esta reciprocidad, entre dignidad y privacidad, que se llega a estimar que el derecho a la vida privada es uno de los derechos más cercanos a la dignidad, al proteger el desarrollo de la libre personalidad de todo individuo. Como señala José María Desantes: "La personalidad en su sentido ontológico incluye ese ámbito amurallable de la intimidad"[16].

Desde el punto de vista normativo, la primera vez que se reconoce explícitamente la noción de dignidad como fuente inspiradora de los derechos del hombre es en la Declaración Universal de los Derechos Humanos[17] del año 1948. Con posterioridad a su proclamación, surgen

[16] DESANTES, José María. 1991. El derecho fundamental a la intimidad. En: Seminario "El derecho a la intimidad y a la vida privada y los medios de comunicación social", 28 de agosto de 1991. España, Centro de Estudios Públicos. 276p.

[17] La Declaración Universal de los Derechos humanos señala en el artículo 1°: "Todos los seres humanos nacen libres e iguales en dignidad y derechos y, dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros".

paulatinamente numerosos tratados y convenciones[18] destinados a reconocer y desarrollar el valor de la dignidad, declarando en consecuencia, una serie de derechos a nivel constitucional como, por ejemplo, el derecho a la vida privada. De hecho, todo Estado que se considere social y democrático debe tener como fin el resguardo y promoción de la dignidad.

En Chile, nuestra Constitución Política de la República reconoce la dignidad en el artículo 1 "Las personas nacen libres e iguales en dignidad y derechos", mientras que en la Constitución Española la dignidad es reconocida en su artículo 10 "La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamentos del orden político y de la paz social".

En ambas constituciones, la dignidad se menciona de forma inaugural, ya que es considerada, como se señala anteriormente, principio rector y generador de los demás derechos humanos, presupuesto y límite del ejercicio de las potestades públicas y fuente integradora de las falencias o lagunas existentes en el ordenamiento jurídico. Por estos motivos, entender

[18] Destacan al respecto el Pacto Internacional de Derechos Civiles y Políticos de 1966 y la Convención de Naciones Unidas contra la Tortura de 1984.

la noción de dignidad es trascendente en el estudio del derecho a la vida privada pues ante las amenazas que surgen contra la privacidad de los individuos y ante la carencia de una norma legal, recurrir al principio de la dignidad, por ejemplo, es una alternativa. En palabras del profesor Lautaro Ríos:

> "En supuestos eventuales que afecten en grado de privacidad, perturbación o amenaza, atributos o requerimientos de la persona no configurados como derechos o garantías, pensamos que puede recurrirse a la noción de dignidad de la persona y a la del libre desarrollo de su personalidad, para reclamar medidas de protección o de restablecimiento, según el caso, del respeto debido por todos a esa dignidad"[19].

1.2. Principales características.

Antes de proceder al estudio de las principales particularidades de este derecho, es primordial realizar ciertas precisiones respecto al término de vida privada y derecho a la vida privada. Gran parte de la doctrina utiliza de

[19] RÍOS A., Lautaro. 1984. La dignidad de la persona en el ordenamiento jurídico español. En: XV Jornadas Chilenas de Derecho Público, 19 al 21 de octubre de 1984. Chile, Universidad de Valparaíso, Facultad de Ciencias Jurídicas, Económicas y Sociales. 206p.

forma intercambiable ambos conceptos, sin embargo, cabe precisar que tienen significaciones distintas. "El primero puede ser concebido como un concepto sociológico y psicológico, 'lo privado o íntimo'. En cambio lo segundo es el instrumento jurídico normativo, que se crea para proteger ese ámbito reservado"[20].

El derecho a la vida privada ha llegado a ser considerado una noción difusa ante la dificultad de otorgar un concepto jurídico claro, unitario y perfectamente delimitado del mismo. Lo anterior es consecuencia de dos de sus principales características señaladas de forma unánime por parte de la doctrina: el carácter relativo y heterogéneo de este derecho.

Por una parte, la relatividad se refleja en el hecho de ser considerada una noción que varía en el tiempo, desde un punto de vista social y cultural, como describe Novoa Monreal:

> "La noción general de vida privada queda determinada, en cierta medida, por los diferentes regímenes sociales, políticos y económicos que existen en el mundo. Estos responden a concepciones diversas

[20] VIAL, Tomás. 2000. Hacia la construcción de un concepto constitucional del derecho a la vida privada. Persona y Sociedad 14(3): 47-68.

del hombre y de la sociedad y se basan en modelos ideológicos discrepantes, que conducen a una apreciación diversa de lo que han de ser las relaciones de un ser humano con otro y de lo que deben ser las relaciones del individuo con la sociedad"[21].

Por otro lado, su carácter heterogéneo es consecuencia de ser considerado un concepto relativo. La heterogeneidad se percibe en la dificultad de plantear un concepto inequívoco de vida privada y, por ende, la imposibilidad de delimitar sus límites de protección de forma concreta. Por este motivo se presenta el peligro de confusión con otros derechos de la personalidad que tienen cierta conexión con la vida privada[22], pero que, sin embargo, tutelan aspectos diferentes de la personalidad de un individuo. En virtud de lo anterior, el profesor Christian Suárez señala "la necesidad de plantear un concepto más específico de este derecho, de manera que sea posible una delimitación clara con otros, que teniendo cierta conexión con

[21] NOVOA M., Eduardo. Derecho a la vida privada y Libertad de Información. Óp. Cit. 43p.

[22] Como ocurre con el derecho al honor y a la propia imagen. Sin embargo, desarrollaremos sus diferencias en el Capítulo II de esta memoria.

los de vida privada o intimidad, manifiestan una construcción lógica y jurídica distinta"[23].

Pese a que reconocemos el riesgo de confusión planteado anteriormente, concordamos con Novoa Monreal en el "rechazo de un concepto absoluto de vida privada, con límites y contenidos fijos e inmutables. Es preciso aceptar, por consiguiente, que se ha de trabajar con un concepto multiforme, variable e influido por situaciones contingentes de la vida social"[24].

En efecto, el carácter relativo de este derecho es considerado por cierto sector de la doctrina como una ventaja en virtud de su dinamismo y flexibilidad. A modo de ejemplo, el catedrático Jijena Leiva fundamenta esta posición señalando que el derecho a la privacidad, al ser considerada una categoría amplia y flexible, permite ofrecer un marco unitario para el tratamiento de una serie de problemas conexos que van surgiendo por el paso del tiempo[25]. En la misma línea argumentativa, el profesor español Martínez de Pisón afirma que la ductilidad de este derecho permite valorar

[23] SUÁREZ, Christian. 2000. El concepto de la vida privada en el derecho anglosajón y europeo. Revista Derecho de Valdivia (11):103-120.
[24] NOVOA M., Eduardo. Derecho a la vida privada y Libertad de Información. Óp. Cit. 44p.
[25] JIJENA, Renato. 1992. La protección penal de la intimidad y el delito informático. Santiago, Editorial Jurídica de Chile. 40p.

una serie de situaciones que fluctúan en el tiempo. Lo que ahora puede parecer perteneciente al ámbito íntimo, más tarde, sin embargo, se hace algo habitual y público[26].

En consecuencia, la relatividad conceptual del derecho a la vida privada resulta sumamente útil para proteger la privacidad de las personas en toda época y lugar, ya que por un lado extiende sus límites de protección ante nuevas amenazas impensadas por el legislador y, por otro, se adapta al cambio de paradigma entorno a lo que se considera público y privado en cada sociedad y cultura.

1.3. Evolución conceptual y doctrinal.

1.3.1. Generalidades.

En nuestra tradición jurídica continental, diversas son las denominaciones conceptuales que recibe este derecho, destacando principalmente la utilización de términos tales como derecho a la privacidad, derecho a la intimidad o derecho a la vida privada a modo de ejemplo.

[26] MARTÍNEZ DE PISÓN, José. 1996. Vida privada e intimidad: implicaciones y perversiones. Anuario de Filosofía del Derecho (14):717-738.

En Chile, nuestra Constitución Política de la República hace referencia al concepto de derecho a la vida privada, mientras que en España su Carta Fundamental hace mención al derecho a la intimidad. En virtud de lo anterior, surge la disyuntiva respecto a si estamos hablado del mismo derecho o, por el contrario, se trata de derechos con una configuración jurídica distinta.

Quienes han defendido la diferencia entre vida privada e intimidad[27] fundamentan su posición al señalar que la intimidad es merecedora de un mayor resguardo jurídico en comparación a la vida privada. Así, Cea Egaña relaciona el derecho a la intimidad con el resguardo de los datos sensibles de las personas, tales como, la orientación sexual, vida conyugal, entre otras, mientras que el derecho a la vida privada tendría relación con informaciones que no son tan sensible, pero que siguen siendo hechos o circunstancias que tiene al titular de ellas como único y exclusivo interesado en mantenerla bajo reserva, confidencia o secreto[28].

[27] Postura compartida por Nogueira Alcalá, Cea Egaña y Gastón Gómez.
[28] FIGUEROA, Rodolfo. 2015. Privacidad. Santiago, Editorial Universidad Diego Portales. 30p.

Por el contrario, la doctrina mayoritaria[29], a la cual adhiere esta tesis, utiliza indistintamente los vocablos de vida privada, privacidad e intimidad, sin entrar en mayor fundamentación conceptual, al estimar que –desde un punto de vista jurídico– no es trascendental realizar una diferenciación terminológica, pues no existen criterios analíticos para apoyar la distinción. Al respecto, Rodolfo Figueroa fundamenta lo anterior al señalar lo siguiente:

> "Si la intimidad es más restringida que la privacidad, ¿ella también tiene límites? Si en ocasiones se pueden alzar las barreras de la privacidad, ¿también se pueden alzar las de la intimidad? La respuesta debe ser negativa para que tenga sentido la distinción. De lo contrario, si cada vez que está autorizado invadir la privacidad lo está también invadir la intimidad, la distinción se torna irrelevante"[30].

Sin embargo, es necesario señalar que, desde el punto de vista semántico, son palabras con significados distintos: "vida privada, o

[29] Entre los autores adeptos a esta postura destacan: Novoa Monreal, Corral Talciani y Jijena Leiva.
[30] Ibíd. 46p.

privacidad e intimidad no son lo mismo, aunque tengan un nexo común"[31]. En concordancia con lo anterior, la Real Academia Española (RAE), en el sentido común de la palabra, define lo privado como aquella parte de la vida "que se ejecuta a vista de pocos", mientras que intimidad corresponde a "la zona espiritual y reservada de una persona o de un grupo, especialmente de una familia"[32]. En efecto, la intimidad y lo privado se consideran "círculos concéntricos de los que la intimidad es el más interior, recóndito y nuclear que lo simplemente privado"[33]. Por este motivo la privacidad está más cerca del mundo corriente, mientras que la intimidad lo está de la conciencia[34].

En nuestro país, queda constancia de esta diferencia semántica, a nivel jurídico, en nuestras Actas Constituyentes, en palabras de Jaime Guzmán:

> "El concepto de privacidad envuelve el ámbito de una de la vida de a persona que debe quedar precisamente excluida de la noticia o de la invasión externa. La intimidad es todavía una zona más profunda y

[31] MARTÍNEZ DE PISÓN, José. Vida privada e intimidad: implicaciones y perversiones. Óp. Cit. 719p.
[32] REAL ACADEMIA ESPAÑOLA. 2014. Diccionario de la lengua española. Intimidad. 23ª ed.[en línea] <http://lema.rae.es/drae/?val=privado> [consulta: 20 enero 2015].
[33] BLÁZQUEZ, Niceto. 2000. El desafío ético de la información. España, Editorial Edibesa. 210p.
[34] GÓMEZ, Gastón.2005.Derechos fundamentales y recurso de protección. Santiago, Ediciones Universidad Diego Portales. 317p.

sensible que la privacidad. Es algo más sutil, y por lo tanto, de menos alcance en su extensión"[35].

Por su parte, España, la derogada Ley Orgánica 5/1992 de Regulación automatizada de los datos de carácter personal señalaba:

"La intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de las personas (…) La privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que este tiene derecho a mantener reservado"[36].

De este modo, la relación de vida privada e intimidad desde el punto de vista semántico es de género a especie[37], por ende son nociones que se encuentran íntimamente ligadas, como señala Martínez de Pisón: "No hay

[35] VIAL, Tomás. Hacia la construcción de un concepto constitucional del derecho a la vida privada. Óp. Cit. pp. 47-48.

[36] España. Jefatura de Estado. 2000. Ley Orgánica 5/1992: De regulación del Tratamiento automatizado de los datos de carácter personal. Vigente hasta el 14 de enero de 2000.

[37] Francia en su Código Civil realizó esta distinción al usar el término de la "intimidad a la vida privada".

intimidad sin vida privada, sin el lugar domestico donde recluirse aún más. Como tampoco hay privacidad, ni se puede gozar de una vida privada sin algo de intimidad"[38].

En opinión de esta investigación, la denominación jurídica elegida por nuestro país –derecho a la vida privada– es más idónea y coherente que la denominación utilizada por el legislador español. De este modo, vida privada, al ser un concepto más amplio que intimidad, refleja de una mejor forma la mutabilidad y flexibilidad del concepto en comento, al extender los límites jurídicos de protección a un mayor número de situaciones, en cambio la denominación utilizada por la normativa española, hace alusión explícitamente al bien jurídico protegido, el cual es la intimidad.

1.3.2. Principales criterios conceptuales.

Diversos han sido los intentos por parte de la doctrina y la jurisprudencia a fin de dilucidar los criterios a considerar para la construcción de un concepto de derecho a la vida privada y establecer los límites de su protección. Grandes son las dificultades, pues, como señala el profesor Pérez Luño: "Las nociones de intimidad y vida privada llevan consigo una

[38] MARTÍNEZ DE PISÓN, José. Vida privada e intimidad: implicaciones y perversiones. Óp. Cit. 721p.

gran carga emotiva que las hace equivocas, ambiguas y dificulta la precisión de su significado"[39].

A continuación, procederé a desentrañar una serie de conceptos y clasificaciones que por su aporte doctrinal resultan de vital importancia en la construcción jurídica de este derecho. En virtud de lo anterior, se analizará, para tales efectos, tres criterios que considero principales:

- El primer criterio consiste en intentar definir la vida privada, en virtud de la delimitación de su contrario, la vida pública.
- El segundo criterio agrupa a todos los autores que buscan otorgar una definición descriptiva de la vida privada, delimitando de forma concreta sus alcances.
- El tercer criterio agrupa a todos aquellos que no buscan otorgar una definición de vida privada, sino que describen los diversos hechos y situaciones con el fin de delimitar el contenido de la vida privada.

[39] PÉREZ LUÑO, Antonio. 2012. Los derechos humanos en la sociedad tecnológica. España, Editorial Universitas. 327p.

En cuanto al primer criterio, hay quienes han llegado a considerar que lo privado se define por oposición a lo público, como si fueran términos antónimos. En esta línea, R. Badinter afirma que la noción de vida pública es más restringida y sus límites más fáciles de determinar y cree que al proceder así se acentúa que la vida privada es lo común y la vida pública la excepción[40]. Si seguimos la lógica de esta postura, lo público se define en razón de "lo que interesa –o debiera interesar– a todos los ciudadanos, los asuntos del Estado y lo que está a disposición de cualquiera"[41]. Si hiciéramos el intento de otorgar una definición de vida privada, con base en lo anterior, seguimos teniendo los mismos problemas conceptuales de siempre.

En efecto, lo público y lo privado no son nociones dicotómicas, tampoco una es común y la otra excepción, sino que, por el contrario, son términos íntimamente ligados, razón por la cual se dificulta aún más establecer sus deslindes. Reafirmando lo anterior, acertadas son las palabras de Martínez de Pisón, quien señala que lo público y lo privado "son espacios, territorios,

[40] BADINTER, Robert. 1968. Le droit au respect de la vie privée. JCP G, vol. 2136, Citado en: NOVOA M., Eduardo. Derecho a la vida privada y Libertad de Información. Óp. Cit. 33p.
[41] GAZITÚA, M., SALINAS, C. y STANGE HANS, M. 2004. Intimidad y vida privada. Santiago, Centro de Estudios de la Comunicación, Universidad de Chile. 3p.

que se interpenetran. Espacios cambiantes en cada momento y situación, hasta el punto que una misma acción puede considerarse pública, privada o íntima con solo variar el cómo y el dónde se realiza"[42].

Es más, ante el progreso de las nuevas tecnologías de la información, los límites entre lo público y lo privado son más difusos que en épocas anteriores y además adquiere relevancia el reconocimiento de una expectativa de privacidad, la cual está presente incluso en espacios considerados públicos y, como veremos más adelante, también en internet.

El segundo criterio agrupa a todos los autores que buscan entregar de forma concreta un concepto de vida privada, a través de la descripción y delimitación de sus alcances. Estiman que solo de esta forma se pueden evitar confusiones con otros derechos, al otorgar una delimitación estricta del derecho a la vida privada. Esta concepción tiene su origen en la frase elaborada por el Juez Cooley: "*The right to be left alone*".

Dentro de los exponentes de esta posición destaca Emilio Pfeffer al definir vida privada como "el derecho a poder estar solo si uno lo desea, mantenerse apartado de la observación de los demás sin ser molestado sin

[42] MARTÍNEZ DE PISÓN, José. Vida privada e intimidad: implicaciones y perversiones. Óp. Cit.721p.

intromisiones en lo más personal de su vida"[43]. Por su parte, para Vial Solar corresponde a "aquel derecho que está destinado a proteger la dignidad y libertad humana, por medio del reconocimiento a su titular de un poder de control sobre su ámbito privado, que en su núcleo central se identifica con el cuerpo y la afectividad, y respecto a la información relativa a la persona"[44]. Mientras que para Corral Talciani "es la posición de una persona (o entidad colectiva personal) en virtud de la cual se encuentra libre de intromisiones o difusiones cognoscitivas de hechos que pertenecen a su interioridad corporal y psicológica o a las relaciones que ella mantiene o ha mantenido con otros, por parte de agentes externos que, sobre la base de una valoración media razonable, son ajenos al contenido y finalidad de dicha interioridad o relaciones"[45].

Si bien se ha de considerar meritoria la intención de otorgar una definición jurídica de este derecho, al conceder un entendimiento general de

[43] PFEFFER, Emilio. 1985. Manual de derecho constitucional. Santiago, Editorial Jurídica Ediar Conosur, Tomo I. Citado en: SUÁREZ, Christian. El concepto de la vida privada en el derecho anglosajón y europeo. Revista Derecho de Valdivia 11: 103-120. Óp. Cit. 107p.

[44] VIAL, Tomás. Hacia la construcción de un concepto constitucional del derecho a la vida privada. Óp. Cit. 68p.

[45] CORRAL, Hernán. Configuración jurídica del derecho a la privacidad I. Óp. Cit. 347p.

la noción de privacidad, estimo que no es lo más adecuado, en razón de los siguientes argumentos:

- La construcción de una definición estricta de este derecho es arbitraria, pues el criterio a seguir se basa únicamente en la voluntad del teórico respecto a lo que él considera privado y digno de protección, por ende, no podemos ahondar en detalle respecto a los argumentos que tuvo en mente, y menos tener certeza en cuanto a las situaciones que él considera una amenaza a la privacidad.

- Se utilizan expresiones carentes de un contenido en concreto[46]. Por ejemplo, no hay claridad respecto de lo que se debe entender por intromisión, poder de control o ámbito privado.

- La vida privada es una noción dinámica y flexible, por lo tanto otorgar un concepto con contenidos fijos simplemente conlleva al riesgo de caer en la obsolescencia.

Para finalizar, el tercer criterio está conformado por aquellos autores que consideran imposible otorgar un concepto de vida privada, por tanto, la

[46] SUÁREZ, Christian. El concepto de la vida privada en el derecho anglosajón y europeo. Óp. Cit. 107p.

solución radica en desentrañar el significado de la privacidad desde la agrupación de una serie de hechos o circunstancias.

A continuación, se destacan tres exponentes, que, en opinión de esta investigación, han realizado aportes trascendentes a esta posición.

W. L. Prosser[47] realiza un detallado análisis de la jurisprudencia norteamericana recaída en esta materia, identificando una serie de hechos ilícitos transgresores de la privacidad, concluyendo que existen cuatro formas generales de invadir el derecho a la privacidad, a saber: i) La intrusión (espionaje o allanamiento de morada), ii) revelación (publicación de fotografías indecorosas), iii) falsa imagen (utilizar un nombre para apoyar una campaña pública) y iv) apropiación de elementos personales para el propio beneficio (nombre, imagen, etc.).

En virtud de lo anterior, la contribución de Prosser radica en otorgar claridad a nivel doctrinal y jurisprudencial respecto a lo que comprende el derecho a ser dejado solo, descrito por Warren y Brandeis en su famoso

[47] PROSSER, William. 1960. Privacy (a legal analysis). Estados Unidos. California Law Review 48(383).

artículo, al agrupar y analizar los diversos casos conocidos por los tribunales norteamericanos en virtud de la transgresión a la *privacy*.

En segundo lugar, destaca la doctrina alemana, por elaborar la teoría de la triple esfera, otorgando una noción del derecho a la vida privada desde una perspectiva de configuración gradual. Esta teoría admite tres graduaciones representadas por círculos concéntricos que van del mayor a menor[48]:

- *Privatsphäre*: la esfera social, la cual comprende todos aquellos comportamientos, noticias y expresiones que el sujeto desea que no lleguen al conocimiento público en general.

- *Vertrauensphäre*: la esfera privada, la cual abarca lo que el sujeto participa a otra persona de confianza; quedando excluidas el público en general y aquellas personas que operan en la vida privada y familiar.

- *Geheimsphäre*: considerada la esfera íntima o del secreto, que corresponde a las noticias y hechos que por su carácter

[48] NOVOA M., Eduardo. Derecho a la vida privada y libertad de información. Óp. Cit. 38p.

extremadamente reservado han de quedar inaccesibles a todos los demás.

La doctrina alemana destaca por tratar de abordar el problema de delimitación de los márgenes del derecho a la vida privada, además de poner en manifiesto la diferenciación entre lo privado y lo íntimo de una forma metódica y clara.

En último lugar, Novoa Monreal[49] estima que la noción de privacidad debe ser definida considerando una serie de factores culturales y sociales del momento. A propósito de esto, señala una serie de características que considera pertenecientes a la vida privada, las que permitirían determinar si algo debe o no considerarse incluido dentro de ese ámbito. Estas características son:

- Que se trate de manifestaciones o fenómenos que normalmente quedan sustraídos al conocimiento de personas extrañas o cuando menos ajenas al círculo familiar del sujeto, o de sucesos que no se desarrollan normalmente a la vista de dichas personas;

[49] Ibíd. pp.49-50.

- Que los hechos referidos son de aquellos cuyo conocimiento por otros provoca normalmente al sujeto una turbación moral en razón de ver afectado su sentido del pudor o recato;
- y, que el sujeto no quiere que otros tomen conocimiento de esos hechos.

El profesor Novoa Monreal, desde la generalidad, nos otorga parámetros para analizar si una situación específica corresponde al ámbito de la vida privada o no. Dicho razonamiento ha llegado a ser considerado en nuestros tribunales superiores de justicia[50], y por tanto, ha permitido estructurar el concepto de derecho a la vida privada, en consideración a nuestra realidad nacional y social.

De lo anterior podemos colegir que ante la problemática de otorgar una noción unificada del concepto de derecho a la vida privada, cada país debiese hacer el intento, a nivel de doctrina y jurisprudencia, de definir los parámetros actuales de protección a la privacidad en virtud a su realidad

[50] El Tribunal Constitucional acoge la doctrina de Eduardo Novoa, reconociendo la existencia de una expectativa de privacidad en los espacios públicos. Rol N° 1984-2011 cuyo Considerando Vigesimotercero señala: "Que la intimidad no solo puede darse en los lugares más recónditos, sino que también se extiende, en algunas circunstancias, a determinados espacios públicos donde se ejecutan específicos actos con la inequívoca voluntad de sustraerlos a la observación ajena".

social y cultural. Para tales efectos, es trascendental sistematizar las diversas categorías de privacidad tanto a nivel doctrinal como jurisprudencial, pues solo de esta forma podremos llegar a comprender con mayor agudeza en qué consiste el derecho a la vida privada, evitando cualquier noción específica que pudiera llevar a una distorsión en la identificación del bien jurídico protegido en cada caso en concreto[51] y, respecto a los cuales, el uso de las TIC se ha transformado en una de las principales amenazas para el este derecho, viéndose afectada principalmente su perspectiva informacional.

2. Derecho a la protección de datos personales.

En concordancia a lo señalado en párrafos anteriores, se reitera que el concepto de privacidad muta en el tiempo en la medida en que la sociedad evoluciona. En los tiempos actuales, el desarrollo tecnológico ha tenido consecuencias impensadas a nivel comunicacional e informacional, produciendo un cambio de paradigma a nivel social, repercutiendo también en la noción de privacidad. En efecto, "si bien la tecnología es neutral, su

[51] FIGUEROA, Rodolfo. 2013. El derecho a la privacidad en la jurisdicción de protección. Revista chilena de derecho 40(3): 859-889.

utilización no lo es"[52]. A partir de esto, surgen nuevas amenazas a la privacidad de las personas, asociadas a la captación y tratamiento indebido de datos de carácter personal mediante el uso de las diversas tecnologías de la comunicación e información, como, por ejemplo, a través del uso de las redes sociales. Atendido lo anterior, se presenta una nueva concepción jurídica del derecho a la vida privada, desde una dimensión informacional, la cual tiene como finalidad la protección de datos de carácter personal.

2.1. Generalidades.

Debemos realizar ciertas precisiones antes de profundizar en el estudio concerniente a la protección de datos de carácter personal. Cuando se hace alusión al derecho a la protección de datos personales, se hace referencia –de forma sinónima– al derecho a la autodeterminación informativa, dado que existe plena coincidencia entre ambos conceptos y la diferencia de denominaciones obedece simplemente a diferencias históricas y

[52] DRUMMOND, Víctor. 2004. Internet, privacidad y datos personales. España, Editorial Reus. 27p.

culturales[53]. Por tanto, en esencia, estamos hablando del mismo derecho, por lo que se utilizará ambas denominaciones de forma homologable. Sin perjuicio de que se estima que la denominación más correcta es derecho a la protección de datos de carácter personal, pues describe de forma concreta el bien jurídico que se pretende resguardar.

En segundo lugar, debemos dejar en claro la discusión doctrinal surgida en torno a la naturaleza jurídica de la protección de datos personales. El debate surge en razón de establecer si el derecho a la protección de datos de carácter personal es un nuevo derecho o, por el contrario, es una proyección del derecho a la vida privada.

Quienes estiman que estamos en presencia de un nuevo derecho, fundamentan su posición al considerar que el tratamiento de datos personales excede al ámbito del derecho a la intimidad, ya que este derecho otorga protección a todo tipo de datos incluso a los que no revisten el carácter de privado según la noción tradicional de intimidad[54].

[53] MURILLO DE LA CUEVA, Pablo. 2008. El derecho a la autodeterminación informativa y la protección de datos personales. Azpilcueta: Cuadernos de Derecho (20):43-58.
[54] Ibíd. 47 p.

A contrario sensu, otro sector de la doctrina[55] considera que la protección de datos personales es una proyección del derecho a la vida privada en su dimensión informacional. En consecuencia, el derecho a la autodeterminación informativa es una forma de referirse a las particulares características que adquiere el derecho a la intimidad en la era informática.

En esta investigación se concuerda con esta última postura, pues, como se ha reiterado, el derecho a la vida privada es multifacético, siendo por tanto solo una de sus diversas expresiones la protección de datos de carácter personal. El derecho a la privacidad en su faceta informacional dota al individuo de una prerrogativa de control sobre los datos e informaciones relativos a su persona[56]. Es necesario precisar que esta prerrogativa de control se otorga sobre todo tipo de datos sin importar su cualidad de público o privado, ya que el derecho a la privacidad informacional se vulnera por la indebida obtención y recopilación de una serie de datos correspondientes a una persona determinada.

[55] NOGUEIRA, Humberto. 2005.Autodeterminación informativa y hábeas data en Chile e información comparativa. Anuario de Derecho Constitucional Latinoamericano 2(11): 449-471; y VALLEJO, Antonio. 1994. Derecho a la intimidad e informática. España, Editorial Comares.

[56] BANDA, Alfonso. Manejo de datos personales. Un límite al derecho a la vida privada. Óp. Cit. 63p.

En efecto, la unificación de datos en bases de datos otorga la posibilidad de construir perfiles detallados de cada individuo, accediendo a información relativa a ciertos rasgos de la individualidad de cada persona, como por ejemplo: estilo de vida, comportamiento e intereses de todo tipo, los cuales pertenecen al ámbito de la privacidad. Como expone Nogueira Alcalá "el respeto a la vida privada o de la intimidad se proyecta en el ámbito de los registros de informaciones manuales e informáticos, que permiten socializar esa información develando ámbitos de la privacidad de las personas"[57].

En vista de lo anterior, el bien jurídico tutelado sigue siendo el mismo, es decir la intimidad, solo que su transgresión se materializa desde una perspectiva distinta y nueva, mediante la captación y tratamiento de datos personales de forma indebida, ya sea porque la captación y recolección de dichos datos se realizó sin el consentimiento de su titular, o, de otra forma, estos datos fueron utilizados con una diversa finalidad a lo consentido por su titular.

En conclusión, aducir que estamos en presencia de un nuevo derecho, simplemente por el hecho de otorgar protección a todo tipo de datos no es

[57] NOGUEIRA, Humberto. Autodeterminación informativa y hábeas data en Chile e información comparativa. Óp. Cit. 451p.

suficiente. Es necesario, como señala Vallejo, reformular la noción del derecho a la intimidad ante esta nueva realidad social y tecnológica[58], mediante la toma de conciencia del aspecto positivo del derecho a la vida privada, lo que equivale al reconocimiento jurídico de su proyección: el derecho a la protección de datos personales.

2.1. Origen histórico y fundamento.

La configuración jurídica de este derecho tiene su origen en la sentencia dictada por el Tribunal Constitucional Federal Alemán en el año 1983, al declarar la inconstitucionalidad de la Ley de Censo de la Población. El Tribunal consideró que los datos solicitados, con motivo del censo, eran excesivos, teniendo una serie de aprensiones respecto al posterior tratamiento que se le pudiese dar a los datos recabados.

En efecto, la combinación de estos datos otorgaba la posibilidad de ser anexados a un individuo determinado, ofreciendo la posibilidad de construir un perfil completo de cada persona encuestada, perdiendo su anonimato y, por ende, transgrediendo su derecho general a la personalidad. Por este

[58] VALLEJO, Antonio. Derecho a la intimidad e informática. Óp. Cit. 48p.

motivo, el Tribunal Constitucional Alemán declaró la inconstitucionalidad de la comentada ley, en razón de la siguiente consideración:

> "El derecho general a la personalidad abarca la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a la propia vida. Por tanto, otorga la libertad de decidir por sí solo sobre la difusión y utilización de los datos personales"[59].

Considerando lo anterior, el Tribunal Constitucional Federal Alemán reconoció a todo individuo el derecho a ser protegido frente al indebido tratamiento informatizado de datos. Además, reconoce en su sentencia como fundamento del derecho a la autodeterminación informativa, el derecho a la dignidad humana y del libre desarrollo de la personalidad[60], constituyéndose el mismo como fundamento moderno del derecho a la

[59] ALEMANIA. 1983. Tribunal Constitucional. Sentencia de 15 de diciembre, 1983 publicada En: BJC Boletín de Jurisprudencia Constitucional. 1984. Madrid, Publicaciones de las Cortes Generales. Traducción por Manuel Daranas.

[60] Debido que en Alemania el derecho a la privacidad no está reconocido explícitamente, los recurrentes contra la Ley de Censo Alemana invocaron el derecho a la dignidad humana y el derecho al libre desarrollo de la personalidad, los cuales emanan del derecho general a la personalidad. En razón de estos derechos, se construye jurídicamente el derecho a la autodeterminación informativa.

privacidad. Es de vital importancia señalar que el Tribunal Constitucional Federal fundó su sentencia en el derecho general de la personalidad por motivo de no estar consagrado explícitamente el derecho a la vida privada en su legislación, siendo esta la causa principal por el cual el Tribunal alemán construyó jurídicamente el derecho a la autodeterminación informativa.

Con posterioridad a la sentencia alemana, el derecho a la autodeterminación informativa empieza a tener reconocimiento progresivo en el mundo[61], como consecuencia de la creciente preocupación de los diversos organismos internacionales y Estados soberanos respecto al tratamiento de datos personales. Esta preocupación se ve acrecentada, en nuestros días, por el avance tecnológico donde almacenar y difundir grandes bases de datos ya no es una tarea compleja, por lo que los datos personales están expuestos cada vez a mayores riesgos.

[61] Carta Fundamental de Portugal de 1976, Constitución de los Países Bajos de 1983, Constitución de la República Federativa de Brasil de 1988, Carta Fundamental de Suecia de 1990, Constitución Política de Colombia de 1991, Constitución Política del Perú de 1993, Constitución de la Nación Argentina de 1994 y otras.

2.2. Concepto.

Antes de proceder al esclarecimiento conceptual del derecho a la protección de datos personales, es pertinente realizar ciertas precisiones en relación al derecho a la vida privada, pues se ha señalado de forma reiterada, la protección de datos de carácter personal es una dimensión más en la configuración jurídica del derecho a la privacidad.

El derecho a la vida privada distingue dos aspectos a considerar en la precisión de esta noción. Por un lado, tenemos su aspecto negativo, el cual se relaciona con el derecho a ser dejado solo, excluyendo del conocimiento ajeno aquellos hechos o circunstancias personales que solo develará el individuo si así lo determina, consintiendo expresamente en ello. Lo anterior se circunscribe a la noción tradicional del derecho a la privacidad, desarrollado en detalle en la primera parte de este capítulo. Por ende, nuestra atención se centrará en el desarrollo del aspecto positivo de este derecho, en cuya virtud el individuo titular del derecho está dotado de una prerrogativa de control sobre los datos e informaciones relativos a su

persona[62]. Aspecto trascendente en nuestros días, en este sentido señala Herminia Campuzano:

> "La realidad actual resulta bien distinta; la excesiva, incontrolada y, en algunos casos, injustificada recolección automatizada de los datos de carácter personal, así como el mal uso que en determinadas ocasiones los organismos públicos y privados pueden hacer de ellos, origina que el individuo pueda ver totalmente cercenado su derecho a la vida privada"[63].

Es en razón del aspecto positivo del derecho a la vida privada mediante el cual se pretende dar protección a las personas contra la recolección y tratamiento indebido de sus datos de carácter personal. Es importante tener claro que lo tutelado jurídicamente no son los datos en sí mismos, sino el valor intrínseco que ellos representan en lo concerniente a la privacidad del individuo[64].

[62] BANDA, Alfonso. Manejo de datos personales. Un límite al derecho a la vida privada. Óp. Cit. 63p.
[63] CAMPUZANO, Herminia. 2000. Vida privada y datos personales: su protección jurídica frente a la sociedad de la información. España. Editorial Tecnos. 83p.
[64] DRUMMOND, Víctor. Internet, Privacidad y Datos personales. Óp. Cit. 49p.

En efecto, como establece la Teoría del Mosaico, postulada por Madrid Conesa, no todos los datos concernientes a una persona son de importancia para el derecho a la intimidad, sin embargo, la unificación de estos datos otorga un marco general de la personalidad de un individuo, el cual se encuentra amparado por el derecho a la intimidad. "Al igual que ocurre con las pequeñas piedras que forman mosaicos, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significados"[65]. Por ejemplo, el nombre como dato aislado no es información privada, sin embargo, si asociamos otros datos a una persona determinada, puede ser esta la puerta de entrada para acceder a lo más íntimo de su persona y en consecuencia, transgredir su intimidad.

En este contexto, y para terminar de precisar la noción en comento, se hará mención a cuatro conceptos elaborados por parte de la doctrina chilena y española respecto al derecho a la protección de datos personales.

Por parte de la doctrina nacional, el profesor Jijena Leiva señala que el derecho la protección de datos personales reside en "la posibilidad de que los ciudadanos titulares y propietarios de los datos que le conciernan

[65] MADRID, Fulgencio. 1984. Derecho a la intimidad, informática y Estado de Derecho. España, Universidad de Valencia. 45p.

controlen el uso y eventual abuso de los antecedentes que a su respecto sean recopilados, procesados, almacenados y cruzados computacional y telemáticamente"[66], mientras que, por su parte Nogueira Alcalá lo define como "el conjunto de normas jurídicas destinadas a asegurar a las personas el respeto de sus derechos, especialmente del derecho a la vida privada e intimidad ante el tratamiento automatizado de los datos personales"[67]. Por parte de la doctrina española, Morales Prats estima que es "la facultad de control sobre datos e informaciones del individuo en la sociedad tecnológica[68]" y para finalizar, Murillo de la Cueva, formula la siguiente definición que, en opinión de esta investigación, es de las más elaboradas por parte de la doctrina:

> "El derecho a la autodeterminación informativa consiste en "El control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no, para preservar de este modo y en último extremo la propia identidad,

[66] JIJENA, Renato. La protección penal de la intimidad y el delito informático. Óp. Cit. 40p.
[67] NOGUEIRA, H. Autodeterminación informativa y hábeas data en Chile e información comparativa. Óp. Cit. 451p.
[68] MORALES, Fermin. 1984. Protección de la intimidad: delitos e infracciones administrativas. Cuadernos de Derecho Judicial 13:39-86. Citado en; PRIETO, María Jesús. 2004. Objeto y naturaleza jurídica del derecho fundamental a la protección de datos personales (I), Boletín del Ministerio de Justicia Español, (58):127.

nuestra dignidad y libertad. En su formulación como derecho implica necesariamente poderes que permitan a su titular definir los aspectos de su vida que no sean públicos, que desea que no se conozcan, así como facultades que le aseguren que los datos que de su persona manejan terceros informáticamente son exactos, completos y actuales, y que se han obtenido de modo leal y lícito[69]".

A grandes rasgos, es posible concluir que el elemento esencial del derecho a la autodeterminación informativa es otorgar a los titulares de los datos de carácter personal, la facultad de control de sus datos. Sin embargo, como bien se desprende de la definición otorgada por Murillo de la Cueva, no es suficiente otorgar una facultad de control si no existen mecanismos jurídicos que permita materializar y coaccionar las transgresiones a la privacidad de los individuos. En consecuencia, es mediante el establecimiento del *habeas data* donde se materializa el derecho a la protección de datos de carácter personal.

[69] DE LA CUEVA, Lucas. 1993. Informática y protección de datos personales (estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal). Centro de Estudios Constitucionales. Citado en: MARTÍNEZ, Ricard. 2007. El derecho fundamental a la protección de datos: perspectivas. Revista D´Internet, Dret I Política (5):49.

2.3. Habeas data.

Siguiendo la lógica de estudio del presente capítulo, a continuación se hará referencia, a grandes rasgos, a las principales características del *habeas data,* con la finalidad de otorgar una visión general de la protección jurídica de datos de carácter personales. En consecuencia, la profundización normativa se analizará en los siguientes dos capítulos al momento de referirnos a la realidad jurídica de Chile y luego a la de España.

El *habeas data*[70] surge como el instrumento legal mediante el cual se asegura, por un lado, el ejercicio del derecho a la protección de datos personales, y por otro impide su transgresión. Como se señala en el apartado anterior, para conceder una efectiva protección a los datos de carácter personal no basta con su reconocimiento legal, sino que es imperioso establecer, además, el mecanismo jurídico mediante el cual se materializa las facultades que otorga este derecho.

Al tenor de lo señalado por Jijena Leiva, "el *habeas data* es una acción cautelar de rango constitucional, heredera de otro recurso y tan importante

[70] En España y gran parte de Europa, la expresión habeas data hace referencia a un proceso que comprende una etapa administrativa y otra judicial. Mientras que en Chile, dicho concepto, se usa solo para referirse a la acción judicial impetrada ante nuestra judicatura.

como el *habeas corpus*[71], que en las modernas sociedades de la información permite a los titulares de los datos personales o patrimoniales, autodeterminar el uso que se haga de sus antecedentes cuando ellos son recopilados, registrados y cruzados computacionalmente"[72].

De acuerdo a la postura que sostengo, el bien jurídico protegido mediante el *habeas data* es la intimidad informacional de las personas, la cual es transgredida mediante la captación y tratamiento indebidos de datos personales. El *habeas data* protege una serie de principios rectores que se encuentran consagrados de forma reiteradas en gran parte de los textos legales de protección de datos de carácter personal a lo largo del mundo y, en consecuencia, presentes en el ordenamiento jurídico chileno. En concordancia con lo anterior, hemos de señalar que, Campuzano Tomé, realiza una clasificación general de estos principios distinguiendo dos momentos fundamentales en la vida del dato: el referente a la captura o

[71] El habeas corpus tiende a proteger la dimensión física y externa de la libertad lo que equivale a nuestro Recurso de Amparo en Chile, mientras que el habeas data protege aspectos internos de la libertad, como lo es la intimidad. PÉREZ LUÑO, Antonio. 1900. Del Habeas Corpus al Hábeas data. En: Conferencia XIV Curso de Informática y Derecho: 11 de mayo de 1900. Toledo, Centro regional de la UNED. pp. 153-161.

[72] JIJENA, Renato. 1999. Dominios, marcas y comercio electrónico en internet: anexo: la nueva ley chilena sobre la no protección de datos personales, Nº 19628 del 28 de agosto de 1999. Informática y derecho: Revista iberoamericana de derecho informático (30): 365-418.

recolección y el momento en que se lleva a cabo el tratamiento o procesamiento. Al respecto, cabe enumerar los siguientes principios generales[73]:

Al momento de la captura o recolección de datos:

- Principio de justificación legal y social.

El cual se traduce en la existencia de un propósito socialmente aceptado, el cual legítima la extracción del dato.

En Chile, podemos sostener que este principio esta implícitamente consagrado en la Ley 19.628 sobre protección a la vida privada del año 1999[74]. A modo de ejemplo, la referida normativa establece que toda persona podrá efectuar un tratamiento de datos en la medida que esté autorizado por la ley o cuente con el consentimiento de su titular[75]. De tal forma, es posible señalar que el titular de los datos personales puede dar su consentimiento a terceros para que estos los recolecten y traten, debido a que dicho actuar es una manifestación de la libertad y voluntad inherente a

[73] CAMPUZANO, Herminia. Vida privada y datos personales: su protección jurídica frente a la sociedad de la información. Óp. Cit. pp.83-84.
[74] Profundizaremos en el estudio de esta ley en el Capítulo II de la presente memoria.
[75] CHILE. Ley 19.628. artículo 4.

todo ser humano y, en consecuencia, aceptado desde una perspectiva social y jurídica.

- Principio de licitud y limitación de la colecta.

La recolección de datos debe ser realizada por medios lícitos y acotados. La recolección será lícita cuando es realizada con el conocimiento y consentimiento del titular de los datos de carácter personal, por ende, los medios empleados no podrán ser fraudulentos, desleales o ilícitos, debiendo especificarse el propósito de recolección de aquellos datos. Será acotada la recolección, cuando la extracción de los datos sea mínima, tan solo los necesarios para cumplir con la finalidad perseguida.

En nuestro país, si bien la Ley 19.628 exige obtener el consentimiento del titular de los datos para su tratamiento, la actual normativa no exige que este consentimiento sea previo y expreso. Lo anterior, tiene como consecuencia que el conocimiento que tiene el titular del tratamiento de sus datos sea deficiente y, además, se vea dificultada la comprobación de que los medios empleados para su extracción sean lícitos.

- Principio de fidelidad de la información.

Los datos deben ser completos, exactos e iguales. Para cumplir con esta finalidad deben estar consagrados en el ordenamiento jurídico el derecho a la rectificación y actualización de los datos.

En Chile, este principio se encuentra explícitamente contenido en el artículo 6 de la Ley 19.628 estableciendo como obligación al responsable del banco de datos, la eliminación, modificación o bloqueo de los datos en caso de que estos sean erróneos, equívocos o incompletos, sin necesidad de requerimiento de su titular.

- Principio de pertinencia y finalidad.

Solo se recolectarán los datos que resulten adecuados para el propósito perseguido en su obtención. Por tanto, serán guardados en los archivos respectivos con el único propósito de utilizarlos para la finalidad prevista.

En cuanto a la realidad de Chile, como señala Alberto Cerda, el principio de finalidad informa persistentemente el contenido de la Ley 19.628, ya que no solo tiene cabida al instante de verificarse la recogida de datos, sino que se extiende a toda operación que recaiga sobre los mismos[76]. Asimismo, el

[76] CERDA, Alberto. 2003. La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales. Tesis para optar al grado de Magister. Santiago, Universidad de Chile. Escuela de Derecho. 89p.

artículo 9 de la Ley 19.628 también reconoce este principio al señalar que los datos personales deben utilizarse solo para los fines para los cuales hubieren sido recolectados.

Al momento del tratamiento o del procesamiento de la información:

- Principio de confidencialidad de los datos recolectados.

Las personas responsables de bases de datos tienen la obligación de guardar secreto y no divulgar el contenido de dichos datos.

Chile consagra este principio en el artículo 7 de la Ley 19.628, especificando, además, dicho deber de confidencialidad se extiende, al responsable de la base, aun después de haber terminado sus actividades en ese campo.

- Principio de seguridad.

Las personas responsables de los bancos de datos, deberán adoptar las medidas necesarias para garantizar la seguridad de los datos, evitando alteraciones, pérdidas, tratamientos o accesos no autorizados.

Nuestro ordenamiento jurídico no reconoce en la Ley 19.628 este principio, si bien impone al responsable del registro o banco de datos el

deber de cuidar de ellos con la debida diligencia, no ha prestado atención alguna en cuanto a medidas concretas que han de aplicarse para brindar un adecuado nivel de cuidado a los datos y prevenir la ocurrencia de tales daños[77].

- Principio de caducidad.

Los datos personales no deben tratarse ni mantenerse archivados más allá del tiempo necesario para cumplir con su finalidad, lo que se traduce en el derecho a cancelación que tienen los titulares de dichos datos y el cual se encuentra reconocido en el artículo 6 de la Ley 19.628 al señalar que los datos deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o haya caducado.

- Principio del consentimiento del afectado.

El principio básico sobre los que se articulan la mayor parte de los sistemas generales de protección de datos de carácter personal. Supone un derecho de información, que resulta aplicable en todo proceso de extracción, tratamiento y disposición del dato personal, siendo un deber para quien pretende recabar el dato.

[77] Ibíd. 95p.

Si bien la Ley 19.628 no define que se debe entender por consentimiento, este principio está reconocido a lo largo del articulado señalando, por regla general, que el consentimiento debe ser expreso y por escrito, sin perjuicio que establece una serie de excepciones que permiten ese tratamiento sin consentimiento de su titular. Sin perjuicio lo anterior, como bien se previno con anterioridad, no consta la obligación de que este consentimiento sea previo, por lo que la reforma en tramitación viene en subsanar esta materia con el fin de establecer una legislación que esté en concordancia con los principales principios a nivel internacional relativos a la protección de datos personales.

Complementando los principios anteriormente señalados, el Consejo Económico y Social de las Naciones Unidas[78], hacemos mención a un importante principio, el cual otorga eficacia y coerción a todo régimen legal de protección de datos personales:

- Control y sanciones.

Debe existir una autoridad que, conforme con el sistema jurídico interno, controle el respeto de los principios ya señalados. Esta autoridad deberá ser

[78] NOGUEIRA, Humberto. Autodeterminación informativa y hábeas data en Chile e información comparativa. Óp. Cit. 452p.

imparcial e independiente respecto a las personas u organismos responsables del tratamiento de datos y de su utilización y tener la adecuada competencia técnica. Debiendo preverse las sanciones penales o de otro tipo y los recursos individuales independientes.

De lo anterior se infiere que para otorgar una efectiva protección a la privacidad y datos personales, todo ordenamiento jurídico que se considere democrático y con un estándar de privacidad adecuado debe plasmar aquellos principios en sus textos legales y establecer un régimen de recursos como ocurre con la consagración del *habeas data*[79]. Sin embargo, para que el sistema legal sea verdaderamente eficaz, estimamos que debe existir un órgano autónomo de control dotado de potestades fiscalizadoras y coercitivas cuya finalidad sea velar por el correcto cumplimiento en la captación y tratamiento de datos personales. De esta forma, si bien el ordenamiento jurídico chileno, a través de la Ley 19.628, reconoce una serie de derechos al titular de los datos personales e impone ciertas obligaciones a los responsables del banco de datos y del registro, reiteramos que en Chile no existe una autoridad pública de control de tratamiento de datos personales, ni sanciones penales para las infracciones serias a la

[79] Ibíd. 451p.

normativa[80]. En consecuencia, este principio no se está cumpliendo en nuestro país.

[80] ONG Derechos Digitales. La privacidad en el sistema legal chileno. [en línea] <https://www.derechosdigitales.org/wp-content/uploads/pp-08.pdf>[consulta: 29 de noviembre 2015]

II. LA PROTECCIÓN A LA VIDA PRIVADA Y DATOS PERSONALES EN CHILE.

Todo Estado que se considere democrático debe asegurar el libre desarrollo de la personalidad de los individuos. Para tales efectos, el fortalecimiento a nivel normativo y social del derecho a la protección de datos de carácter personal y del derecho a la privacidad es trascendental para el cumplimiento de este propósito. Lo anterior se vuelve una necesidad imperiosa en la época actual, debido al vertiginoso desarrollo de las TIC que tienen como consecuencia el surgimiento de nuevas y numerosas amenazas contra la privacidad de las personas.

El mayor desarrollo normativo en privacidad y protección de datos personales se encuentra arraigado a la tradición anglosajona y europea, sirviendo ambos modelos como fuente de inspiración en el desarrollo jurídico interno de cada Estado latinoamericano. En el caso de Chile, es el modelo europeo y, en específico, la normativa proveniente de España y de la Unión Europea, nuestro principal parámetro a seguir en materia

normativa y en la implementación de diversas políticas públicas, con la intención de cumplir con un estándar adecuado de privacidad.

El estándar adecuado de privacidad, siguiendo a Raúl Arrieta[81], es aquel que concede una efectiva protección a la vida privada de las personas, mediante la articulación de un sistema jurídico coherente y, además, comprenda la instauración de diversos mecanismos tendientes a tutelar la efectividad del cumplimiento de estas disposiciones legales.

Dentro de este este contexto, se ha señalado que Chile no cumple con un estándar adecuado de privacidad, destacando como principal motivo el no contar con una autoridad de protección de datos. En efecto, como señala Alberto Cerda, "la obtención de un nivel de protección adecuado para los derechos fundamentales de las personas concernidas por el tratamiento de datos supone, imprescindiblemente, incorporar en nuestra normativa una autoridad de control especialmente avocada a velar por el cumplimiento de la misma[82]."

[81] ARRIETA, Raúl. 2009. Chile y la protección de datos personales: Compromisos Internacionales. En: ¿Están en crisis nuestros derechos fundamentales?, Serie de Políticas Públicas. Chile, Ediciones Universidad Diego Portales. pp. 1-12.
[82] CERDA, Alberto. 2003. La autoridad de control. Óp Cit. 89p.

En razón de lo anteriormente señalado, en el presente capítulo se ha de analizar, a grandes rasgos, la experiencia chilena en lo concerniente a privacidad y protección de datos de carácter personal, así como las principales falencias respecto al régimen sancionatorio y coercitivo de nuestra actual normativa.

1. Experiencia nacional.

1.1. Generalidades.

En Chile, el derecho a la vida privada es una garantía fundamental consagrado en los artículos 19 N° 4 y N° 5 de la Constitución Política de la República de 1980. Por otro lado, la consagración a nivel legal del derecho a la privacidad se encuentra en la Ley 19.628 de 1999 sobre vida privada y protección de datos de carácter personal.

Es necesario señalar que la actual normativa ha perdido eficiencia y eficacia, debido al vertiginoso avance de las tecnologías de la información y comunicación. Lo antedicho se manifiesta de tal forma, que tanto en la Constitución Política de la República como en la Ley 19.628, se han detectado una serie de falencias que impiden a nuestro país cumplir con el estándar adecuado de privacidad. En efecto, como señala Raúl Arrieta:

> "La ley permite e incentiva, en abierta contradicción con su espíritu, ciertas estrategias que posibilitan la vulneración de los derechos supuestamente amparados por la misma, sin considerar sanciones para los responsables del tratamiento de datos personales que infringen la ley; igualmente la acción judicial prevista para la protección del derecho no cumple estándares de aseguramiento del principio del debido proceso que debe regir a los procedimientos judiciales. A ello se suma que el sistema de información a los ciudadanos es insuficiente y que no se cuenta con una autoridad de control, lo que redunda en que las personas, que diariamente se ven afectadas por la forma en que se tratan sus datos personales, muchas veces abusivamente, tanto por parte de organismos públicos como privados, ni siquiera conocen o dimensionan cuáles son sus derechos ni cómo se ejercen[83]."

Como consecuencia de lo anterior, se procederá a analizar las principales normas referentes a la privacidad contenida tanto en la Constitución Política

[83] ARRIETA, Raúl. 2009. Chile y la protección de datos personales: Compromisos Internacionales. En: ¿Están en crisis nuestros derechos fundamentales? Óp. Cit. 21p.

de la República como en la Ley 19.628, pues solo de esta forma se comprenderá los próximos desafíos que tiene Chile respecto a esta materia.

1.2. Constitución Política de la República.

El artículo 19 N°4 de nuestra Constitución Política de la República de 1980, reconoce a todas las personas "el respeto y derecho a la protección a la vida privada[84]", mientras que el N° 5 de dicho artículo asegura "la inviolabilidad del hogar y de toda forma de comunicación privada. El hogar solo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley".

La redacción del comentado articulado estuvo a cargo de la Comisión de Estudios de la Nueva Constitución Política de la República (CENC), mayormente conocida como Comisión Ortúzar. Es preciso señalar que dicha comisión consideraba unificar en un mismo numeral el derecho a la vida privada e inviolabilidad del hogar y de toda forma de comunicación privada. Sin embargo, por decisión del Consejo de Estado, se procedió a dividir en dos numerales las referidas disposiciones, lo cual se ha de

[84] Antes de la reforma constitucional del año 2005 se reconocía a nivel constitucional la protección de la vida pública.

considerar desafortunado y carente de fundamento, pues tanto el N° 4 y N° 5 del artículo 19 de la Constitución Política de la República, protegen diversos aspectos de la privacidad. Mientras el artículo 19 N° 4 hace referencia a la noción general de vida privada desde una perspectiva intangible, el N° 5 corresponde a la proyección material del referido derecho, el cual se manifiesta en el resguardo del hogar y de toda forma de comunicación privada, dos elementos de gran importancia para el legislador a lo largo de los años y de fácil comprobación mediante los sentidos. Así, el N°5 hace referencia a una noción negativa de privacidad, al otorgar el derecho a repeler a terceros de ciertos elementos que tienen existencia material en nuestro mundo, y que simbolizan la privacidad que todo ser humano desea y debe tener. Mientras que el N° 4, como bien se ha mencionado, es la consagración general del derecho a la vida privada y, en consecuencia, se ve protegido tanto el aspecto negativo, como positivo de este derecho. Este numeral es trascendental, pues permite adecuar su interpretación a un determinado momento social y cultural, ya que se debe recordar que el concepto de privacidad es dinámico y mutable.

Ahora, respecto a lo que se debe entender por privacidad en nuestro país, la CENC optó por no especificar dicho concepto a nivel constitucional, pues

consideraba que la vida privada "es un rubro en el cual difícilmente se pueden establecer líneas demasiado precisas desde un punto de vista general y va a tener que ser la jurisprudencia la que vaya sentando, en cierto modo, la doctrina sobre este punto"[85]. Siendo, por tanto, la judicatura la cual ha profundizado y delimitado el alcance de esta noción, destacando para estos efectos la sentencia dictada en el Caso Martorell, al definir la noción de privacidad en el siguiente tenor:

> "Se viola la vida privada y origina las sanciones que establezca la ley, la intrusión indebida y maliciosa en asuntos, comunicaciones o recintos íntimos que el titular del bien jurídico protegido no desea que sean conocidos por terceros sin su consentimiento, se cause o no con tal motivo sufrimiento o daño al afectado[86]".

La acción de protección[87], como mecanismo jurídico de protección a los derechos consagrados en el artículo 19 N° 4 y N° 5 de la Constitución

[85] Chile. 1980. Historia de la ley: Artículo 19 N° 4 de la Constitución Política de la República: El derecho a la privacidad. 24p.
[86] ONG Derechos Digitales. La privacidad en el sistema legal chileno. [en línea] <https://www.derechosdigitales.org/wp-content/uploads/pp-08.pdf> [consulta: 29 de noviembre 2015]. 27p.
[87] Destinada a amparar el libre ejercicio de las garantías constitucionales enumeradas en el artículo 20, mediante la adopción de medidas de resguardo necesarias ante un acto u omisión arbitrario o ilegal que impida, restringa o perturbe ese ejercicio.

Política de la República, es insuficiente. En efecto, a diferencia del sistema español, nuestra judicatura no exige el agotamiento de la vía judicial ordinaria para poder impetrar la referida acción. Esto tiene como consecuencia la inexistencia de una oportunidad procesal detallada para exponer y probar los hechos en los cuales basan sus alegaciones los recurrentes. Además, existe desconocimiento por parte de los recurrentes en cuanto a los alcances de la noción de privacidad y sus diversas proyecciones.

Lo anterior tiene genera que en aquellos casos donde corresponde alegar la transgresión de las garantías reconocidas en el artículo 19 N° 4 y/o N° 5 de la Carta Fundamental, los recurrentes no las invocan o, si llegan a hacerlo, simplemente hacen mención al articulado sin entrar en mayor fundamentación, impidiendo a los Tribunales Superiores de Justicia referirse sobre este tema ante el peligro de incurrir en *ultra petita*.

Debido al procedimiento establecido para impetrar la acción de protección, gran cantidad de casos son rechazados únicamente en base a argumentos formales, sin considerar el fondo del asunto. De tal forma, son escasas las ocasiones en que la judicatura ha podido razonar y, en

consecuencia, construir criterios a nivel jurisprudencial en materia de privacidad.

No es de extrañar que el derecho a la privacidad presente dificultades para su delimitación por entrar en confusión con otros derechos, como ocurre con el derecho al honor[88] y a la propia imagen. Que, si bien manifiestan una construcción lógica y jurídica distinta, desde un punto de vista fáctico se encuentran directamente vinculados.[89]

En razón de lo anterior, se procederá a analizar, a grandes rasgos, el desarrollo normativo del derecho a la vida privada en Chile y su estrecha relación con los conceptos de inviolabilidad del hogar, de las comunicaciones privadas y el derecho a la propia imagen. De esta forma se podrá comprender y reconocer los parámetros de protección a la privacidad en Chile y, así, constatar la creciente necesidad de contar con nuevos

[88] La vida privada se vulnera mediante la simple toma de conocimiento de forma indebida de aspectos reservados a la esfera privada de un individuo y de su familia, aun cuando el transgresor esté de buena fe. Al contrario, se transgrede la honra de una persona y de su familia, mediante la difamación pública con la intención de causar un agravio mal intencionado. En Chile el derecho a la vida privada está garantizado a todas las personas por igual, en cambio el derecho a la honra no. Pues toda persona tiene derecho a un grado de honra, pero ese grado varía entre los individuos. Como bien consta en las actas de la CENC, "en la medida que cada uno con su conducta agrega honor, va incrementando su honra y por lo tanto, su derecho a la honra".

[89] SUÁREZ, Christian. El concepto de la vida privada en el derecho anglosajón y europeo. Óp. Cit.1p.

mecanismos e instituciones tendientes a reforzar y educar en materia de privacidad y protección de datos personales a los individuos de nuestro país.

i) Derecho a la vida privada.

Se considera que la actual Constitución Política de la República de 1980 innovó en materia de privacidad al otorgar respeto y protección de forma explícita en el artículo 19 N° 4 al derecho a la vida privada y en el N° 5 a la inviolabilidad del hogar y de las comunicaciones privadas.

Con el transcurso de los años, nuestra Carta Fundamental ha sufrido diversas reformas, destacando en esta materia la modificación en el año 2005 del artículo 19 N° 4, que en su redacción original también consagraba el respeto y protección de la vida pública[90].

Respecto al concepto de vida privada, la CENC decidió utilizar esta denominación para consagrar este derecho, al considerar que dicho concepto estaba más arraigado en el lenguaje común utilizado en nuestro país.[91] Además, dicho concepto también abarcaría la noción de intimidad.[92]

[90] Se optó por reformar dicho numeral suprimiendo la consagración constitucional del delito de difamación y, por ende, la protección a la vida pública

[91] Chile. Historia de la ley: Artículo 19 N° 4 de la Constitución Política de la República: El derecho a la privacidad. Óp Cit. 32p.

La Comisión optó por una redacción concisa en el articulado, al considerar las múltiples amenazas que podrían surgir en el futuro contra la privacidad de las personas, entregando a la jurisprudencia la labor de sentar doctrina en esta materia.[93] Empero, como se ha señalado con anterioridad, no ha sido fácil el ejercicio de esta labor por parte de los Tribunales Superiores de Justicia, sin perjuicio de que en la sentencia dictada en el Caso Martorell se otorgó una definición de privacidad, basada en la definición entregada por el profesor Cea Egaña[94], en el siguiente tenor:

> "Se viola la vida privada y origina las sanciones que establezca la ley, la intrusión indebida y maliciosa en asuntos, comunicaciones o recintos íntimos que el titular del bien jurídico protegido no desea que sean conocidos por terceros sin su consentimiento, se cause o no con tal motivo sufrimiento o daño al afectado[95]".

---

[92] VIAL, Tomás. Hacia la construcción de un concepto constitucional del derecho a la vida privada. Óp. Cit. 48p.
[93] Ibíd. 48p.
[94] CEA EGAÑA, José Luis. 1996. El derecho constitucional a la intimidad. Revista Gaceta Jurídica, (198):27.
[95] ONG Derechos Digitales. La privacidad en el sistema legal chileno. [en línea] <https://www.derechosdigitales.org/wp-content/uploads/pp-08.pdf> [consulta: 29 de noviembre 2015]

En cuanto a lo que debemos entender por respeto y protección a la vida privada de acuerdo a los términos del artículo 19 N° 4 de la Constitución Política de la República, el mismo catedrático señala:

> "El respeto es la obligación de los terceros en orden a acatar los valores jurídicos –vida privada, vida pública y honra–, mientras que protección es el conjunto de medios (acciones, peticiones recursos, actuaciones y decisiones) que el ordenamiento jurídico reconoce al titular de esos bienes jurídicos para defenderlos, hasta exigir y obtener que sean respetados"[96].

Respecto a lo que se debe entender por respeto y protección de la vida privada de la persona y su familia, en virtud de lo estipulado en el artículo 19 N° 4 de la Constitución Política de la República, Cea Egaña señala:

> "El respeto es la obligación de los terceros en orden a acatar los valores jurídicos –vida privada, vida pública y honra–, mientras que protección es el conjunto de medios (acciones, peticiones recursos, actuaciones y decisiones) que el ordenamiento jurídico

[96] CEA EGAÑA, José Luis. 1993. Misión cautelar de la Justicia Constitucional. Revista Chilena de Derecho. 20 (2-3):395-408.

reconoce al titular de esos bienes jurídicos para defenderlos, hasta exigir y obtener que sean respetados"[97].

Dentro de este contexto y, con la intención de reforzar el respeto y protección de la vida privada en dicho numeral, es importante señalar que se encuentra en tramitación el reconocimiento a nivel constitucional del derecho a la protección de datos personales[98], debido a la creciente preocupación que conlleva el impacto de las tecnologías de la información y comunicación, a la esfera privada de las personas.

De aprobarse la referida reforma, se incorporarían los siguientes párrafos segundo y terceros a la redacción actual del artículo 19 N° 4:

> "Asimismo, la protección de sus datos personales, el derecho a acceder a ellos y a obtener, en la forma que determine la ley, su rectificación, complementación y cancelación, si estos fueren erróneos o afectaren sus derechos. El tratamiento, circulación y traspaso de esos datos deberá realizarse en la forma y condiciones que fije la ley".

[97] CEA EGAÑA, José Luis. Misión cautelar de la Justicia Constitucional. Óp. Cit. 440p.
[98] Boletín N° 9384-2007 el cual consagra el derecho a la protección de datos personales.

Esta memoria estima, que por motivos de considerar al derecho a la protección de datos personales como una proyección del derecho a la vida privada y, como tal, ya se encuentra protegido a nivel constitucional en virtud del artículo 19 N° 4 y N° 5° de la Constitución Política de la República. La reforma en tramitación no deja de ser beneficiosa, ya que refuerza la protección y delimitación del derecho a la privacidad mediante el reconocimiento explícito de su ámbito informacional, concerniente a la protección de datos de carácter personal.

De tal forma, de aprobarse la reforma, se "refrendaría el criterio de nuestro Tribunal Constitucional, el cual, siguiendo la tendencia jurisprudencial de varias altas cortes europeas, ha elevado a la calidad de derecho fundamental de la protección de datos personales"[99].

ii) Derecho a la propia imagen.

De acuerdo a lo señalado en las actas de la CENC, nunca se discutió la posibilidad de consagrar de forma explícita el derecho a la propia imagen, pues la comisión consideró que el derecho a la vida privada consagrado en artículo 19 N°4 "cubriría también la posibilidad de captación de

[99] Boletín N° 9384-2007 que Consagra el derecho a la protección de datos personales. 2p.

imágenes"[100]. Sin embargo, esta investigación adhiere a la posición doctrinal, que considera al derecho a la vida privada y derecho a la propia imagen como derechos autónomos, que poseen una configuración jurídica diversa[101].

El derecho a la propia imagen se define mediante la explicación de sus dos dimensiones, una positiva y otra negativa. La primera dimensión, la positiva, faculta a la persona a captar, reproducir y publicar su propia imagen; mientras que la segunda, correspondiente a la dimensión negativa, otorga el derecho a impedir que un tercero no autorizado, cualquiera sea su finalidad, capte, reproduzca y/o publique la imagen de otra persona[102], siendo el aspecto negativo de este derecho el que constantemente entra en confusión con el derecho a la privacidad.

La principal diferencia entre el derecho a la vida privada y el derecho a la propia imagen, estriba en el ámbito de protección de este último; ya que lo que se pretende proteger "no es que la persona venga a ser conocida en

[100] Chile. Historia de la ley: Artículo 19 N° 4 de la Constitución Política de la República: El derecho a la privacidad. Óp. Cit. 42p.
[101] NOVOA, Eduardo. Derecho a la vida privada y Libertad de Información. Óp. Cit. 66p.
[102] NOGUEIRA, Humberto. 2007. El derecho a la propia imagen como derecho fundamental implícito: fundamentación y caracterización. Ius et Praxis 13 (2): 245-285.

sus hechos íntimos, sino que su apariencia o rasgos distintivos sean utilizados para fines ajenos a su interés"[103].

Dentro de este contexto, es posible hacer las siguientes aseveraciones:

- Se vulnera el derecho a la vida privada y no el derecho a la propia imagen; en todos aquellos casos en que se capta, se reproduce y/o difunde, de forma indebida, un hecho perteneciente a la esfera privada de una persona. En efecto, la captación o difusión de la imagen es solo un medio para violar el derecho a la privacidad[104].
- Por exclusión, se vulnerará el derecho a la imagen y no el derecho a la vida privada, en todos aquellos casos en que dicha difusión no se realice con la finalidad de denostar a una persona o publicitar ciertos aspectos de su vida privada. Por tanto, se transgrede el derecho a la imagen en todos aquellos casos en que la imagen de otra persona es utilizada, en la generalidad de los casos, con fines patrimoniales.

El derecho a la propia imagen ha adquirido relevancia jurídica en nuestra época, en virtud del auge que ha vivido las TIC en estos últimos años. El

[103] CORRAL, Hernán. 2001. La vida privada y la propia imagen como objetos de disposición negocial. Revista de Derecho (8):159-175.
[104] NOVOA, Eduardo. Derecho a la vida privada y Libertad de Información. Óp. Cit. 71p.

acceso general a la tecnología por parte del público en general ha permitido la utilización masiva de diversos aparatos tecnológicos que permiten captar imágenes y videos de forma instantánea; mientras que el acceso a internet y, en específico, la utilización de las redes sociales ha permitido la difusión masiva de imágenes. Lo anterior, tiene como consecuencias que tanto el derecho a la propia imagen como el derecho a la vida privada se vean gravemente amenazados.

De acuerdo a lo anteriormente expuesto, ante las dificultades presentes en nuestra época, relacionadas con cómo controlar el uso indebido de la imagen ajena y ante el peligro de coartar el derecho fundamental a la libertad de información y comunicación, reconocido en el artículo 19 N° 12 de la Constitución Política de la República, la protección al derecho a la propia imagen se ha empezado a manifestar como un derecho de índole negativa.

El aspecto negativo del derecho a la propia imagen se proyecta ante la posibilidad de su titular de manifestar su rechazo expreso a que su imagen sea conservada por otros, a falta de este rechazo expreso ha de entenderse que cualquiera puede captar imágenes ajenas en lugares públicos, sin otra

restricción que las necesarias para el respeto de otros derechos del hombre[105].

En la actualidad, en Chile se ha pretendido otorgar protección al derecho a la propia imagen, mediante una interpretación extensiva del artículo 19 N° 4. Lo cual, adelanto, se ha extendido en el ámbito de las redes sociales.

En virtud de lo anteriormente expuesto, estimo que este derecho debiese estar consagrado de forma explícita y autónoma en nuestra Constitución Política de la República, ya que, como se ha señalado, el derecho a la propia imagen tiene una configuración distinta al derecho a la vida privada y al honor.

iii) Derecho a la inviolabilidad del hogar y de las comunicaciones privadas.

La Constitución Política de la República de 1925 en su artículo 10 N° 12 consagraba la inviolabilidad del hogar y en el N° 13 la inviolabilidad de la correspondencia epistolar y telegráfica, las cuales eran consideradas una emanación del derecho a la propiedad[106].

[105] Ibíd.
[106] CHILE. Congreso Nacional. 2009. Historia de la Constitución Política, artículo 19 N°4. Sesión N° 129, junio 1975. 19p.

En la actual Constitución, se mantuvo la consagración de estas garantías, pero, a diferencia del texto anterior, el fundamento de su consagración radicó en ser consideradas una proyección del derecho a la vida privada desde una perspectiva material y no del derecho a la propiedad, como se pensaba en tiempos anteriores. En efecto, la CENC consideró que tanto la inviolabilidad del hogar y de la correspondencia corresponderían a dos proyecciones inmediatamente ligadas al ser íntimo de una persona[107], siendo esta la razón por la cual se mantiene la protección a nivel constitucional de estas dos instituciones.

Dentro de este contexto, surgió la redacción del artículo 19 N° 5, el cual asegura a todas las personas:

> "La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar solo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinadas por la ley".

Esta perspectiva material del derecho a la privacidad es la que cuenta con un mayor grado de protección a nivel normativo. En efecto, el derecho

[107] Ibíd. pp. 17 y ss.

a la inviolabilidad de hogar se ve reforzado tanto en el código penal al regular las sanciones contra la vulneración de secretos y su divulgación (art. 161 a) como en el código procesal penal al regular la entrada y registro de lugares tanto públicos como privados (arts. 205, 206, 222, 303, entre otros).

Respecto al derecho a la inviolabilidad del hogar, como se mencionó, este corresponde a la proyección territorial[108] del derecho a la vida privada y no del derecho a la propiedad, pues se protegen distintos bienes jurídicos. En efecto, "lo que se respeta en esta inviolabilidad es el santuario de la persona, y no cabe por tanto confundirla con el derecho de propiedad, de manera que el hogar es inviolable exista o no dominio sobre el inmueble en el cual está instalado"[109].

[108] Se refiere a la fijación de límites a la intromisión en los espacios o medios domésticos y otros tales como el centro laboral o, incluso, el espacio público. En este contexto, las nuevas tecnologías tienen un gran impacto a través de los medios de registro de información que, debido al nivel de miniaturización, conectividad y ubicuidad existente, son capaces de inmiscuirse en la esfera privada de las personas, considerando su domicilio, sus conductas en lugares públicos y en su lugar de trabajo, sin filtro ni límites. Se vincula a la vida privada y a la inviolabilidad del hogar y de las comunicaciones privadas.
ONG DERECHOS DIGITALES. La privacidad en el sistema legal chileno. [en línea] <https://www.derechosdigitales.org/wp-content/uploads/pp-08.pdf pp13>[consulta: 29 de noviembre 2015]

[109] VIAL, Tomás. Hacia la construcción de un concepto constitucional del derecho a la vida privada. Óp. Cit. 59p.

La CENC, en la redacción de este primer párrafo, decidió utilizar el término hogar como sinónimo de domicilio, ya que consideró que "dicha expresión debe entenderse tal como siempre se ha explicado este precepto: la inviolabilidad favorece al recinto cerrado en que se desarrolla una actividad humana estando negado al acceso de un tercero sin el consentimiento del que está a cargo de él"[110]. Conforme a lo anterior, la noción de hogar comprende el hecho de vivir en un lugar determinado, el de trabajar y, además, el tener control de un reciento privado bajo cualquier título.

A mayor abundamiento, se debe considerar que dicha inviolabilidad no solo protege contra la entrada de forma indebida a un determinado lugar, sino que además, en virtud de las nuevas amenazas contra la privacidad que conlleva el uso de las TIC, esta garantía debe otorgar protección contra cualquier perturbación que puede sufrir una persona en su espacio material, sin que fácticamente se compruebe una intromisión material.

Ahora, en cuanto al derecho a la inviolabilidad de las comunicaciones privadas, la CENC decidió utilizar una denominación amplia para hacer

[110] Chile. Historia de la ley: Artículo 19 N° 4 de la Constitución Política de la República: El derecho a la privacidad. Óp Cit. 17p.

referencia a este derecho; ya que el término de comunicaciones privadas abarcaría, dentro sus límites de protección, toda "correspondencia epistolar, telegráfica, comunicaciones telefónicas y toda otra forma de comunicación que pudiera surgir en el futuro"[111]. Reflejándose, al tenor de lo anterior, la creciente preocupación por parte del legislador de otorgar una efectiva protección a la esfera privada de las personas contra toda amenaza tecnológica, siendo este el motivo fundamental por el cual la CENC redactó de forma escueta la consagración de este derecho, evitando el peligro de la taxatividad, ya que, como se ha señalado, el concepto de privacidad cambia con el transcurso del tiempo, de la cultura y del avance tecnológico.

Sin perjuicio de lo anterior, a nivel doctrinal se ha intentado definir el concepto de comunicación privada, siendo para Silva Bascuñán "aquel tipo de comunicación en que el remitente escoge singularizadamente la persona que la recibe"[112]. Por ende, este derecho otorga la facultad de impedir cualquier intromisión por parte de terceros a los cuales no va dirigida

[111] Ibíd. 30p.
[112] VIAL, Tomás. Hacia la construcción de un concepto constitucional del derecho a la vida privada. Óp. Cit. p. 11.

aquella (comunicación), ya sea bajo la forma de intercepción, abertura o registro"[113].

De lo anterior, es posible aventurarse a concluir que en la medida en que exista algún tipo de filtro y control de la comunicación por parte del emisor que permita singularizar a sus receptores, estaremos en presencia de una comunicación de índole privada y, por tanto, protegida su inviolabilidad a nivel constitucional. Sin embargo, ante la masificación de los medios de comunicación y el desarrollo de internet, establecer el marco diferencial entre comunicaciones públicas y privadas es complicado, sobre todo en las redes sociales. Se tratará sobre este punto en el capítulo V, al analizar en detalle el caso de las redes sociales y la aplicabilidad de la normativa en este ámbito.

Para concluir este apartado, es importante señalar que para otorgar una mayor comprensión del derecho a la privacidad, las garantías reconocidas en el artículo 19 N° 4 y N° 5 de la Constitución Política de la República debiesen estar unificadas en solo un numeral, por motivos de que ambos numerales protegen diversas manifestaciones del derecho a la vida privada.

[113] Ibíd. 63p.

En consecuencia, es procedente excluir el derecho al honor en dichas circunstancias. En efecto, la redacción actual acentúa el peligro de confusión entre ambas garantías que si bien protegen ámbitos inherentes a todo ser humano, el bien jurídico protegido es distinto. No toda violación a la vida privada será una transgresión al honor y viceversa. Además, con la finalidad de reforzar el reconocimiento y protección del derecho a la vida privada, es trascendental consagrar de forma expresa, el derecho a la protección de datos personales pues solo de esta forma, la privacidad informacional tendrá el nivel adecuado de protección que merece a nivel constitucional.

1.3. Ley 19.628.

1.3.1. Generalidades.

La Ley 19.628 sobre protección a la vida privada del año 1999 es la encargada de proteger y regular el tratamiento de los datos de carácter personal de las personas naturales, mediante el establecimiento de normas sustantivas y procedimentales. Chile fue el primer país latinoamericano en promulgar una ley respecto a esta materia.

El objeto de protección de la actual normativa dista de la idea concebida en sus inicios en el proyecto original. En efecto, el proyecto original pretendía consagrar un estatuto general de la protección a la vida privada, el cual tenía por finalidad "llenar un vacío en nuestro ordenamiento jurídico, con el propósito de dar una adecuada protección al derecho a la privacidad de las personas ante eventuales intromisiones ilegitimas, en el ámbito civil"[114]. Lo anterior, siguiendo el modelo español contenido en Ley Orgánica 1/1982 que analizaremos en el siguiente capítulo.

Sin embargo, la Comisión[115] desistió de esta idea, al considerar la complejidad del tema y, por estimar que la acción de protección era un medio idóneo para proteger la vida privada de las personas.

Debido a estos motivos, el proyecto original fue modificado significativamente, conservando solo la regulación de la privacidad desde su perspectiva informacional, promulgándose en consecuencia un estatuto

[114] CHILE. Congreso Nacional. 1999. Historia de la ley 19.628: Artículo 17 sobre protección de la vida privada. Agosto 1999. 100p.

[115] Consta en las actas de la Historia de la Ley que la comisión de Constitución, Legislación y Justicia por unanimidad decide reducir el proyecto, regulando solo la protección de datos personales, al estimar que esta materia es importante para merecer un tratamiento específico. Ampliar el proyecto a la protección de la intimidad de la vida de las personas llevaba a una serie de complejidades que nos ponían, a veces, en contradicción con otra legislación despachada por el Parlamento, como la ley de Prensa. CHILE. Congreso Nacional. Historia de la ley 19.628: Artículo 17 sobre protección de la vida privada. Óp Cit. 142p.

jurídico encargado de proteger y regular específicamente el tratamiento de datos personales.

Es de reconocer que la Ley 19.628 en su época de dictación fue un gran aporte, debido a que reconoció una serie de derechos a los titulares de datos personales y una acción especial para ejercer ante los tribunales en caso de vulneración de estos derechos.

Sin perjuicio de ello, con el transcurso del tiempo y la evolución de las TIC se desvelaron serias falencias presentes en la Ley 19.628[116]. En este sentido, desde que se publicó esta ley, se han presentado más de 70 mociones parlamentarias tendientes a perfeccionar el tratamiento de los datos personales; motivo por cual desde el año 2012 se encuentra en tramitación la reforma de esta ley contenida en el Boletín 8143-03 denominado "Modificaciones a la Ley N° 19.628 'Sobre protección a la vida privada y protección de Datos de Carácter Personal'", la cual pretende reforzar los derechos y protección de datos personales de sus titulares, cumplir con los compromisos adquiridos por Chile en virtud de su

[116] Algunas falencias son: la ausencia de consagración del principio de finalidad y del deber de información en el tratamiento de datos personales, existencia de conceptos que generan dificultades interpretativas, falta de claridad respecto a quien es el responsable del tratamiento de datos, falta de registro de banco de datos privados.

incorporación a la OCDE e incrementar los estándares legales de Chile para transformarlo en un país con un nivel adecuado de protección.

En estas condiciones, se describirá de forma general la evolución de la actual legislación y próximos desafíos que tiene Chile en materia de privacidad y protección de datos personales, por lo que se analizan a continuación los principales aspectos de la Ley 19.628, contrastándolos con la reforma actualmente en tramitación.

1.3.2. Evolución legislativa de la Ley 19.628.

Como se mencionó anteriormente, el proyecto original es muy distinto a la normativa que finalmente se promulgó en la Ley 19.628, la cual solo conservó el nombre del proyecto original "Sobre protección a la vida privada"; denominación que, en opinión de esta investigación, no es del todo correcta, pues la normativa vigente solo regula una de las tantas aristas de la privacidad.

En sus inicios, el proyecto de esta ley, buscaba proteger la vida privada de las personas y sus proyecciones, tales como la intimidad personal y familiar, el anonimato y reserva, la vida tranquila, la inviolabilidad del hogar y de toda forma de comunicación privada y la propia imagen, tanto de

las personas naturales vivas como fallecidas. Además, contemplaba una presunción de ilegalidad relativa a toda intromisión a la vida privada de las personas; dedicando solo el título II a la regulación del tratamiento de los datos personales.

Si bien la actual normativa conserva, en parte, la esencia del proyecto original concerniente a la protección de datos personales; la Ley 19.628 innova al desarrollar un lenguaje técnico a lo largo de este estatuto jurídico, facilitando una correcta comprensión de las normas contenidas en este estatuto jurídico, mediante la definición de una serie de conceptos claves en materia de tratamiento y protección de estos datos.

Como se ha mencionado, pese a que nuestro marco regulatorio fue pionero en Sudamérica al momento de su dictación; el avance vertiginoso de las tecnologías de la información y comunicación han tenido como consecuencia que la presente normativa pierda eficacia en la protección a la vida privada de los individuos, por lo que resulta fundamental reforzar la idea de control que deben tener los titulares de estos datos y así favorecer su protección, frente a toda intromisión de terceros, sean estos públicos o

privados y, por tanto, establecer las condiciones bajo las cuales estos últimos podrán efectuar legítimamente el tratamiento de tales datos.

Es debido a estos antecedentes que surge la necesidad imperiosa de modificar la actual Ley 19.628 y lograr crear un estatuto jurídico que cumpla con el estándar adecuado de privacidad exigido a nivel internacional, sobre todo considerando las directrices estipuladas por la OCDE sobre protección de la privacidad y flujo transfronterizos de datos personales; en virtud del convenio de adhesión que firmó Chile en el año 2011 con esta organización, debiendo cumplir con los principios y la creación de diversos procedimientos e instituciones legales y/o administrativas tendientes a garantizar la protección de la privacidad y las libertades individuales en lo relativo a datos personales, debiendo poner Chile especial empeño en[117]:

- Adoptar una legislación nacional adecuada,

[117] OCDE. 2002. Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales. [en línea] <http://www.oecd.org/sti/ieconomy/15590267.pdf> [consulta: 29 de noviembre 2015]

- Impulsar y apoyar la autorregulación, ya sea mediante códigos de conductas o de otro modo;
- Brindar medios razonables para que los individuos ejerzan sus derechos;
- Sancionar adecuadamente y ofrecer soluciones en caso de fallo; y
- Asegurar la no discriminación desleal hacia el sujeto de datos.

En este contexto, se describirá la actual normativa contenida en la Ley 19.628 y los principales cambios que pretende instaurar el proyecto de modificación de esta ley, analizando para tales efectos cuatro temas esenciales relacionados con esta materia y así esclarecer si nuestro país está bien encaminado en adecuar su normativa a los preceptos consagrados a nivel internacional en materia de protección de datos personales y privacidad en general.

i) Objeto jurídico de protección.

El artículo 1 de la Ley 19.628 señala que el objeto de esta normativa es proteger los datos de carácter personal de las personas naturales, mediante la articulación de un sistema legal que permita proteger sus datos de cualquier tratamiento ilícito o arbitrario, reconociendo para tales efectos una

serie de derechos a los titulares de datos que tienen como fin último dar protección al bien jurídico de la intimidad y, más específicamente, a la autodeterminación informativa[118].

Para efectos de determinar la naturaleza jurídica de los datos a proteger, la presente normativa establece dos categorías; por una parte, los datos de carácter personal, definidos en el articulado como aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables y, por otra, los datos sensibles[119], aquellos que se refieren a 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.

La actual reforma de esta ley mantiene el mismo objeto jurídico de protección, realizando solo modificaciones tendientes a precisar de forma

[118] JERVIS, Paula. 2006. La regulación del mercado de datos personales en Chile. [en línea] <http://www.repositorio.uchile.cl/handle/2250/114258> [consulta 29 de noviembre 2015]

[119] Hemos de mencionar que respecto a este tema ha surgido el Boletín N° 6.994-07 el cual restringe el uso de datos personales de carácter sensibles disponibles en redes sociales en internet. Los cuales no podrán ser utilizados por terceras personas, para otros fines, más que para aquellos, que dentro del contexto doméstico o socializador de la red social, sean utilizados o estén disponibles, a menos que cuente con el consentimiento expreso del titular.

más adecuada el marco técnico y teórico de aplicación de la referida reforma, con la finalidad de favorecer el desarrollo doctrinal y jurisprudencial en materia de protección de datos personales. Para lograr esta propósito, el nuevo artículo 1° busca precisar y reforzar el objeto de protección, enfatizando que se protegen los datos personales, cualquiera sea el tipo de soporte en que consten, que permita su tratamiento por entidades privadas o públicas, vinculando dicha protección con el legítimo ejercicio del derecho de protección a la vida privada, garantizado a todas las personas en el número 4 del artículo 19 de la Constitución Política de la República.

Por tanto, las mejoras residen en reconocer explícitamente a la protección de datos personales como una emanación del derecho a la vida privada y, también establecer un concepto más general al señalar que se protege el tratamiento de datos personales que consten en cualquier soporte, no especificando como ocurre en la actual normativa que utiliza la denominación de registro o banco de datos, la cual no es correcta, pues las bases de datos se estructuran en registros de datos y estos a su vez se almacenan en un soporte el cual puede ser electrónico o físico.

ii) El consentimiento en el tratamiento de datos de carácter personal.

La ley 19.628 determinó que el tratamiento de datos personales solo puede efectuarse cuando la ley u otras disposiciones legales lo autoricen o el titular consienta en ello. Para estos efectos, la ley establece la forma en que debe entregarse este consentimiento, el cual deberá ser expreso y por escrito.

Respecto al tratamiento de los datos sensibles, la regla general señala que estos no pueden ser tratados, excepto en aquellos casos en que la ley lo permite o sean datos necesarios para otorgar beneficios de salud.

Al contrario, la Ley 19.628 también señala que no será necesario requerir autorización para el tratamiento de datos personales, cuando estos provengan o se recolecten de fuentes accesibles al público y cuando dicho tratamiento sea realizado por las personas privadas para el uso exclusivo suyo.

Dentro de este contexto, la reforma en tramitación introduce la gran novedad del consentimiento previo con el objeto de enmarcar la licitud de todo tratamiento de datos personales, requiriendo para tales efectos que la manifestación de voluntad debe ser expresa y efectuarse de manera libre,

inequívoca e informada para que resulte válida, de todos los datos personales que consten en cualquier tipo de soporte.

Respecto a los datos sensibles, el proyecto señala que en concordancia con la experiencia comparada se establece un estándar más exigente, señalando que se pueden tratar este tipo de datos en caso de contar con consentimiento previo, el cual debe ser expreso, previo, específico y no puede constar en cualquier soporte. Debe ser por escrito cuando lo permita la ley o sea necesario para otorgar beneficios de salud. Además, a diferencia de la actual normativa, establece un listado taxativo de excepciones que autorizan el tratamiento lícito de datos personales bajo ciertas circunstancias, que justifican que no medie el consentimiento previo del titular.

La propuesta de consentimiento previo del proyecto de reforma busca que una vez recogidos estos datos el titular de ellos tenga conocimiento posterior de que sus datos son o serán objeto de un tratamiento especialmente autorizado por ley, con el objeto de que pueda ejercer los demás derechos que se le confieren respecto a ellos y que ya han sido objeto

de tratamiento; razón por la cual subsisten las obligaciones que la ley prescribe para el responsable del registro o base de datos.

iii) Derecho de los titulares de datos.

La Ley 19.628 reconoce una serie de derechos a sus titulares, destacando de forma esencial el derecho de acceso o de información, el derecho de modificación o rectificación, el derecho de cancelación y el derecho de oposición, los cuales se infieren reconocidos en toda la normativa de esta ley.

La reforma de esta ley, dentro de sus novedades, define explícitamente los derechos que incorpora, con la finalidad de otorgar un mayor conocimiento y comprensión de ellos a los titulares de los datos personales. Además entrega al Ministerio de Economía, Fomento y Turismo la tarea de crear un reglamento que pasa a regular cada uno de estos derechos, otorgando para dicho fin las definiciones de cada uno. Se ahondará en la naturaleza jurídica de cada derecho al estudiar el caso español, el cual es fuente de inspiración directa de la actual reforma en tramitación:

- Derecho de acceso o información.

Es el derecho del titular para obtener directamente del responsable del tratamiento de datos personales toda información que tiene respecto de su persona.

- Derecho a modificación o rectificación.

Es el derecho del titular de datos personales erróneos, inexactos, equívocos o incompletos, incorporados en una base de datos para que sean modificaciones o actualizados por el responsable de tales datos.

- Derecho de cancelación.

Es el derecho del titular que se ejerce en contra del responsable del tratamiento de datos personales para que se supriman o eliminen los datos personales que vulneren el principio de proporcionalidad.

En forma de adelanto, hemos de mencionar que en el ámbito de las redes sociales es este derecho el cual se transgrede en la generalidad de los casos.

- Derecho de oposición.

Es el derecho del titular que se ejerce en contra el responsable del tratamiento de datos personales y que tiene por objeto impedir que se lleve

a cabo el tratamiento de sus datos de carácter personal o se cede en el mismo.

Como podemos observar, la reforma mantiene la consagración de estos derechos, pero otorga explícitamente el reconocimiento y definición de estos; sin embargo, para complementar el contenido de estos derechos, la reforma contiene un mandato que ordena la promulgación de un reglamento que regule el reconocimiento de estos derechos, lo que correspondería a la misma configuración orgánica presente en la normativa española.

iv) Principios rectores en la protección de datos personales.

Si bien en el capítulo anterior fueron descritos los principales principios que deben regir en la recolección y tratamiento de datos personales; es menester señalar que el proyecto de ley incorpora el reconocimiento explícito de los principios básicos reconocidos por la OCDE[120] con la finalidad de adecuar la normativa contenida en la Ley 19.628 al estándar adecuado de privacidad exigido a nivel internacional. Dichos principios son los siguientes:

[120] OCDE. Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales. [en línea] <http://www.oecd.org/sti/ieconomy/15590267.pdf> [consulta: 17 de noviembre 2015]

- Principio de proporcionalidad.

Los datos de carácter personal solo se podrán recolectar y someter a tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y los propósitos o finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

- Principio de especificación.

El propósito de la recolección de datos personales se deberá especificar en los casos en que se requiera el consentimiento, a más tardar en el momento en que esta se produce, y en cada momento en que se realiza un cambio de propósito.

- Principio de limitación de uso.

El tratamiento de los datos personales se verá limitado al cumplimiento de los propósitos de su recolección, y no se deberán tratar tales datos, excepto si se tiene el consentimiento del titular o lo dispone la ley.

- Principio de seguridad de los datos.

Los responsables del tratamiento de datos personales emplearán las medidas técnicas y organizativas adecuadas a los riesgos que presenta el

tratamiento, tales como pérdida, o acceso, destrucción, uso, modificación o divulgación de los mismos, cuando estas acciones no hayan sido autorizadas.

- Principio de acceso y oposición

El titular o el interesado tienen el derecho a obtener información de todos los datos relativos a su persona que consten en un registro o base de datos, y a oponerse a su tratamiento cuando no haya justificación legal para él.

- Principio de transparencia.

En virtud del cual debe informarse al titular de los datos personales acerca del objetivo del tratamiento y la identidad del responsable del registro o base de datos.

- Principio de información.

El titular tiene derecho a que se le comunique en cada recolección de datos personales, de manera expresa, precisa, clara, inequívoca y gratuita, la información que los responsables del registro de datos deben suministrarle en conformidad a la ley.

Como bien señala el mensaje de la referida reforma, "la introducción de estos principios constituye la implementación de un marco teórico que favorecerá el desarrollo de la doctrina y jurisprudencia en la aplicación concreta de la ley a los conflictos y situaciones vigentes en la sociedad de la información, sirviendo estos principios de elementos de interpretación que actuarán como una bisagra entre la norma jurídica vigente y el valor imperante en una situación determinada"[121]. Lo anterior viene en reforzar y estructurar la tarea pendiente que tiene la jurisprudencia nacional en la regulación de materias relacionadas con la privacidad y, en específico, con la protección de datos de carácter personal.

1.3.3. Control coercitivo y sancionador.

En nuestro país solo existe un control judicial para asegurar el cumplimiento de la normativa contenida en la Ley 19.628 de protección a la vida privada y de los datos de carácter personales, ya que Chile no cuenta con un órgano administrativo que realice un control previo de legalidad, como en la mayoría de los países miembros de la Unión Europea y, por cierto, España.

[121] CHILE. Congreso Nacional. 2011. Mensaje N° 395- 359 del Presidente de la República que modifica la Ley 19.628.

En efecto, durante la tramitación de la ley antes citada se consideró que la tendencia legislativa era prescindir de una autoridad de control en la materia, sobre la base de tres consideraciones, a saber:

> "La proliferación de los micro ordenadores habida durante el decenio de los 80, que ha hecho posible que prácticamente todas las empresas puedan configurar su propio banco de datos; la consiguiente incapacidad de la autoridad central para detectar un empleo inadecuado de los datos contenidos en un fichero tan particularizado; y, finalmente, el creciente movimiento internacional de datos, que dificulta un control centralizado de la exportación de datos personales"[122].

Lo anterior ciertamente es una decisión lamentable, ya que hasta el día de hoy Chile no cumple con uno de los principios esenciales en materia de protección de datos, el cual es tener un sistema de control y sanciones idóneos para asegurar el cumplimiento y protección de los derechos contenidos en la Ley 19.628. Lo anterior se debe a la inexistencia de una autoridad de control imparcial e independiente, que además tenga una

[122] CHILE. Congreso Nacional. 1999. Historia de la ley 19.628: Artículo 17 sobre protección de la vida privada. p. 114.

adecuada competencia técnica en la resolución de conflictos surgidos respecto a esta materia.

En efecto, si bien nuestro ordenamiento jurídico otorga al titular de los datos personales el derecho de impetrar la acción de protección, la ley 19.628, por su parte, reconoce la acción especial de *habeas data*, la cual, como se describió en el capítulo anterior, tiene por objeto otorgar al afectado el derecho a solicitar a la justicia ordinaria, la protección de los derechos supuestamente transgredidos por el responsable de un registro o base de datos.

Sin embargo, el procedimiento de reclamo[123] establecido en la referida ley, al ser un procedimiento judicial, tiene como consecuencia para el afectado ciertos costos asociados en el ejercicio de la referida acción; destacando el costo económico y el tiempo invertido en los tribunales judiciales. Debido a esto, los afectados al analizar el costo-beneficio de impetrar la referida acción en los tribunales deciden no perseverar su accionar en sede judicial, al ser mayores los costos asociados que los beneficios a obtener.

[123] JERVIS, Paula. La regulación del mercado de datos personales en Chile. Óp. Cit. 146p.

En concordancia con lo anterior, Raúl Arrieta señala: "Las dificultades que presenta el recurso de habeas data son muchas, pero solo con fines enunciativos podemos aseverar que tiene problemas para el titular de los datos personales en lo que significa la determinación del tribunal competente, el desigual tratamiento procesal que tienen las partes en el proceso lo que trae implícita la vulneración del debido proceso y la bilateralidad de la audiencia; finalmente, no se establece un plazo de prescripción de la acción con lo que se afecta la seguridad jurídica"[124].

En consecuencia, en el ámbito de las redes sociales, a modo de ejemplo se puede considerar excesivo tener que recurrir a la judicatura por motivo de la denegación del derecho de cancelación por parte de otro usuario en la red social Facebook, lo que ciertamente desincentiva el ejercicio de los derechos reconocidos en nuestra actual normativa.

A mayor abundamiento, la ineficacia e ineficiencia del ejercicio del *habeas data* en Chile se debe a una serie de factores, tales como ignorancia por parte de la ciudadanía en lo referente a temas de privacidad y protección de datos personales, dificultades para probar los hechos reclamados, las

[124] ARRIETA, Raúl. 2009. Chile y la protección de datos personales: Compromisos Internacionales. En: ¿Están en crisis nuestros derechos fundamentales? Óp. Cit. 5p.

sanciones establecidas en la Ley 19.628 que se expresan en penas irrisorias que no incentivan a su cumplimiento y, además, la dificultad de impetrar procesos judiciales en contra de organismos internacionales, tales como, los proveedores de las diversas redes sociales. Todos estos factores tienen como consecuencia que el sistema de reclamo establecido en la referida ley sea ineficaz.

La actual reforma en tramitación, si bien trae consigo grandes avances en materia de protección de datos personales, ha vuelto a omitir la creación de un órgano administrativo autónomo, al pretender otorgar competencia para solucionar conflictos entre privados al Servicio Nacional del Consumidor y, además, realizar ciertas modificaciones al procedimiento establecido ante los tribunales civiles impetrando para tales efectos una especie de sumario especial, y en el caso de los conflictos presentados entre entidades públicas otorgando competencia al Consejo para la Transparencia (en adelante, "CPLT", indistintamente).

Ahora, es preciso señalar que en la cuenta del primer informe[125] de la reforma, diversos expertos en la materia intervinieron y dieron sus

[125] CHILE. Comisión de Economía, Fomento y Desarrollo. Primer Informe. Boletín N° 8.143-2012 de 11 de enero de 2012.

consideraciones respecto a la autoridad que debiese estar encargada de la protección de datos personales. En esta línea, se destaca la intervención realizada por el profesor Renato Jijena, quien señala como aspecto negativo de la referida reforma lo siguiente:

> "Que se pretenda subsanar la inexistencia de un órgano fiscalizador o autoridad de control, asignando competencia al efecto al Sernac en el sector privado y al Consejo de Transparencia en el sector público, sin conferir las competencias y herramientas necesarias a una autoridad autónoma para velar por el adecuado cumplimiento de las normas sobre protección de datos. La Ley 19.628 posee una parte dogmática débil, no tiene parte orgánica, no contempla procedimientos administrativos de tutela sino uno judicial y engorroso, y no posee un arsenal sancionatorio adecuado. Chile sería, de aprobarse esta idea de legislar, el único país del mundo donde la función de autoridad de

control y protección de datos se dividiría entre dos entes per se no idóneos"[126].

Asimismo y, para concluir, como bien expuso Jijena, lo que debe enfatizarse y que está en juego, en el actual debate de la reforma a la ley 19.628, es el tema de defender una garantía fundamental contemplada en el artículo 19 N° 4 de la Constitución Política de la República –el respeto y protección de la vida privada de las personas y sus familias– que legalmente en Chile fue protegida con gran falta de idoneidad el año 1999 por la Ley N° 19.628. Siendo por tanto imperioso contar con una autoridad de control, como lo es una agencia de protección de datos personales en Chile, para así dar eficacia al sistema y, además, cumplir con el estándar adecuado de privacidad en general.

Si bien en un pasado se pretendió reformar la Constitución para crear una agencia de protección de datos, mediante el Boletín 6594-07, dicha propuesta lamentablemente fue archivada[127]. En la actualidad, si bien a

[126] JIJENA, Renato. Comentario al Boletín 8143. [en línea] <http://www.rlpdp.com/2013/03/renato-jijena-leiva-comentarios-al-boletin-8143/> [consulta: 29 de noviembre de 2015]

[127] La comisión lo ha archivado en virtud del artículo 36 bís inciso segundo del Reglamento del Senado: "Transcurrido dos años sin que la comisión se hubiere

nivel de prensa[128] es comentada la intención de Chile de crear una autoridad de control con estas características, en la actualidad el proyecto que busca reformar a la ley 19.628 no ha contemplado su creación.

En opinión de esta memoria, la creación de una autoridad nacional autónoma e independiente es imperioso, pues ante el nuevo escenario que ofrece internet, el conocimiento técnico y normativo que manejan este tipo de autoridades es trascendental para poder adecuar la aplicación de la actual normativa en el ámbito de internet, y en específico de las redes sociales.

En efecto, el pretender otorgar competencia al SERNAC para resolver los conflictos entre privados, considero que no es lo más razonable, ya que por una parte la reforma tampoco le ha de reconocer potestades de oficio, tendientes a reforzar la inspección y control que debe ejercer, así como también estimo que dicha entidad tiene por objeto proteger los derechos de

---

pronunciado sobre los asuntos sometidos a su conocimiento, estos pasarán inmediatamente al archivo."

[128] Proyecto busca que empresas borren datos personales de usuarios. [en línea] Radio Cooperativa en internet. 28 de octubre, 2014. <http://www.cooperativa.cl/noticias/pais/gobierno/proyecto-busca-que-empresas-borren-datos-personales-de-usuarios/2014-10-28/184545.html>[consulta: 24 de enero de 2016]

los consumidores, lo que sin duda es un ámbito totalmente distinto a lo que abarca la protección de los datos personales de los ciudadanos.

Respecto al Consejo de Transparencia, quien deberá resolver los conflictos entre entidades públicas, he de señalar que, si bien considero que lo idóneo es contar con una autoridad de control especializada, ante la imposibilidad inmediata de contar con una entidad de estas características, el CPLT parece ser la opción más razonable, pues ya tiene experiencia resolviendo reclamaciones de acceso a la información pública, y está dotado de un consejo docto en la materia.

Sin embargo, estimo que para que no exista disparidad de criterio entre el SERNAC y el CPLT debiese entregársele la competencia para resolver los conflictos también entre privados al CPLT, así como instar a la predominancia de la labor preventiva.

1.4. Ley 19.733.

Es importante hacer referencia a la Ley 19.733 "Sobre libertades de opinión e información y ejercicio del periodismo", del año 2001, mejor conocida como "Nueva Ley de Prensa", pues es la encargada de regular el tratamiento de los datos de carácter personal que se efectué en el ejercicio

de las libertades de emitir opinión y de informar sin censura previa; no aplicándose en consecuencia la normativa contenida en la Ley 19.628.

El derecho a la vida privada y la libertad de emitir opinión e informar son derechos humanos relativos, pero el primero tiene carácter individual, pues interesa solamente al individuo, mientras que el segundo tiene carácter social y su subsistencia y ejercicio comprometen ciertamente el interés general. La prevalencia del interés público sobre el individual es el fundamento por el cual no se puede censurar de forma previa la libertad de opinión e informar, aun cuando pueda estar en peligro el derecho a la vida privada de una persona; persiguiéndose por tanto *ex posteriori* la correspondiente responsabilidad.

En concordancia con lo anterior, la Ley 19.733 en su artículo 1 asegura el derecho de toda persona natural o jurídica de fundar, editar, establecer, operar y mantener medios de comunicación social, sin otras condiciones que las señaladas por la ley. Mientras que el artículo 2 define como medios de comunicación social, aquellos aptos para transmitir, divulgar, difundir o propagar, en forma estable y periódica, textos, radios, sonidos o imágenes destinados al público, cualquiera sea el soporte o instrumento utilizado

De lo anterior se desprende que por motivos de la redacción general de la definición de medio de comunicación social, sumado a la independencia del soporte utilizado, las redes sociales pueden ser consideradas como un tipo de medio de comunicación social; y por tanto se reconocería de forma explícita el derecho de toda persona natural y jurídica a emitir e informar sin censura previa, también en el ámbito de las redes sociales en virtud de lo reconocido en el artículo 19 N° 12 de la Constitución Política de la República. Sin embargo, se realizará un análisis en mayor profundidad en el capítulo V, al tratar la aplicabilidad de la normativa en el ámbito de las redes sociales.

Como se ha visto, si bien contamos con la consagración a nivel constitucional del derecho a la vida privada, el desarrollo conceptual y la determinación de sus principales alcances y contenidos ha sido escaso por parte de la jurisprudencia; lo que sumado a la perdida de eficiencia y eficacia de la actual normativa contenida en la Ley 19.628 debido al vertiginoso avance de las tecnologías de la información y comunicación, tiene como consecuencia que Chile no cumpla con el estándar adecuado de privacidad exigido a nivel internacional, destacando entre sus motivos la carencia de una autoridad de control que se encargue efectivamente de

fiscalizar el cumplimiento de la normativa, así como de imponer sanciones a los infractores.

Esta autoridad de control debe ser creada *ex novo* a efectos de velar por el adecuado cumplimiento de la normativa concerniente al tratamiento de datos personales. Lo anterior obedece a tres razones esgrimidas por Alberto Cerda y compartidas en la presente memoria: "la primera, reforzar ante las entidades responsables de registros el carácter fiscalizador de la autoridad de control; la segunda, evitar que la sanción a toda infracción deba suponer a intervención judicial; la tercera, la experiencia que se observa en la realidad nacional, en la cual es habitual conferir facultades de tal carácter a la autoridad encargada de velar por el cumplimiento de determinada normativa, así por ejemplo, la Dirección del Trabajo respecto a la legislación laboral y de seguridad social[129]."

[129] CERDA, Alberto. 2003. La autoridad de control. Óp Cit. 219p.

III. LA PROTECCIÓN A LA INTIMIDAD Y DATOS PERSONALES A LA LUZ DE LA EXPERIENCIA ESPAÑOLA.

1. Generalidades.

En España la protección a la intimidad y datos de carácter personal se articula teniendo en consideración, por una parte, la normativa comunitaria de los Estados europeos, destacando la Directiva 95/46 del Consejo de Europa y, por otra, la legislación interna española, la cual consagra a nivel de garantía fundamental ambos derechos. Sin embargo, como bien intuyó el constituyente español, no basta con reconocer el derecho a la intimidad y el derecho a la protección de datos de carácter personal a nivel constitucional, sino se estructura además, un sistema normativo que permita proteger y sancionar la transgresión de estos derechos.

Para estos efectos, con la finalidad de cumplir con el mandato constitucional se promulgaron las correspondientes leyes sectoriales. Así, la Ley 1/1982 de 5 de mayo de 1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, es la encargada de proteger los derechos contenidos en el artículo 18.1 de la Constitución

Española y, posteriormente la Ley 15/1999 de 13 de diciembre de 1999, sobre Protección de Datos de Carácter Personal, tiene la misión de proteger el derecho contenido en el artículo 18.4 de la Constitución.

Asimismo, es importante señalar que para garantizar de forma eficaz los derechos ya mencionados, la labor a nivel administrativo que realiza la Agencia Española de Protección de Datos, en conjunto con la normativa imperante en esta materia, es trascendental; pues dentro de las funciones de esta entidad destacan la fiscalización y protección de los derechos antes mencionados. Sin embargo, se hará referencia en detalle sobre este tema en el próximo capítulo; ya que en este apartado es necesario hacer mención al desarrollo normativo español tanto a nivel constitucional como de las leyes sectoriales para así poder tener una visión general del ordenamiento jurídico español; pues solo de esta forma podremos entender con posterioridad la importancia del rol de la Agencia Española de Protección de Datos en la protección y fiscalización de estos derechos.

2. Principales tratados y convenios.

De acuerdo al artículo 96 de la CE, todo tratado válidamente celebrado por España, una vez publicados oficialmente, formará parte del

ordenamiento interno. De esta norma es posible desprender dos consecuencias trascendentales, por una parte, los tratados internacionales inciden en la configuración jurídica interna de la nación y, por otra, complementan las reglas de interpretación de todos los derechos fundamentales reconocidos a nivel constitucional; siendo este segundo elemento, de vital importancia e influencia en la configuración del derecho a la intimidad en España, pues del mismo modo que en Chile, su construcción conceptual fue entregada a la jurisprudencia de sus Tribunales de Justicia.

En cuanto a los principales tratados y convenios suscritos por España en materia de privacidad y datos personales, destacan la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y la Convención de la OCDE. Además, sobresalen los tratados internacional suscritos por España a nivel regional, debido al fuerte sentido comunitario presente en todo el continente europeo y, de los cuales se procederá a describir, los principales que destacan en materia de intimidad y protección de datos personales.

A nivel regional, las primeras políticas comunitarias tendientes a resguardar el derecho a la intimidad y datos personales, son dictadas por el Consejo de Europa[130], organismo constituido por el Tratado de Londres de 1949. Dicha organización tiene por finalidad establecer un marco de principios y objetivos comunes en toda la región. Dentro de las principales directrices que promulgó para estos fines, destacan dos convenios de vital importancia para el establecimiento de las principales políticas de privacidad a nivel continental.

Estos son el Convenio Europeo para la Protección de Datos (en adelante, "CEDH", indistintamente) de 1950, el cual destaca por reconocer de forma expresa el derecho la vida privada[131] y, el Convenio 108[132] de 1981, el cual es considerado el primer texto internacional que permitió armonizar las leyes de los diversos estados y, en definitiva, el primer paso importante en la elaboración de un armazón legislativo común en el campo de la

[130] Organización internacional destinada a promover la cooperación de los Estados europeos, teniendo como eje rector los valores de la democracia, los derechos humanos y la ley.
[131] Artículo 8: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia".
[132] Este reconoce que "el fin del presente convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de datos de carácter personal".

protección de datos[133]. En efecto, el Convenio 108 fue el encargado de condensar en un cuerpo normativo las principales y más eficientes disposiciones regionales en materia de privacidad y tratamiento automatizado de datos, otorgando los primeros parámetros respecto a lo que se debía considerar como estándar adecuado de privacidad, al reconocer en su normativa comunitaria, una serie de garantías y limitaciones en el tratamiento automatizado de datos a nivel regional.

Tiempo después, con el nacimiento de la Unión Europea en el año 1983 (en adelante, la "UE", indistintamente), se acentúa la intención de los diversos Estados miembros por fortalecer y expandir la protección a la intimidad y datos personales, al buscar garantizar la aplicación sistemática de estos derechos fundamentales tanto en sus estados miembros como en los demás países con los que la UE se relaciona activamente, como es el caso de Chile[134].

[133] CAMPUZANO, Herminia. Vida privada y datos personales: su protección jurídica frente a la sociedad de la información. Óp. Cit. 79p.

[134] La Unión Europea y Chile han tenido una extensa relación bilateral, relación profundizada por la suscripción de un Acuerdo de Asociación en el año 2002, el cual propende a una alianza estratégica para instar al dialogo político, el comercio y la cooperación en general.

En este contexto, surge la principal medida comunitaria[135] en materia de protección de datos personales, la Directiva 95/46/CE, que tiene por finalidad garantizar a cualquier persona natural la protección de sus datos de carácter personal respecto al tratamiento automatizado de estos, destacando el mandato contenido en su artículo 32.1, el cual ordenaba a todos sus Estados miembros a la transposición de su normativa interna con la establecida en la directiva y de esta forma fortalecer y unificar la el derecho a la protección de datos personales a nivel regional.

Además, con el progreso de las tecnologías han surgido diversas directivas que tienen por finalidad complementar y adaptar la actual normativa frente a los nuevos desafíos que conlleva la evolución de las TIC. Para tales efectos, destaca la labor realizada por el grupo de trabajo 29, el cual estuvo encargado de discutir las principales preocupaciones frente a la sociedad de la información, destacando la Directiva 2002/58/CE, modificada en el año 2009, sobre la privacidad y las comunicaciones electrónicas y la directiva 98/34/CE modificada por la Directiva 98/48/CE de Servicios de la Sociedad de la Información, y los Dictámenes 5/2009

[135] La cual surge por consecuencia de las ideas y principios aportados por la UE en colaboración con el consejo de Europa, organismo que desde el año 1995 los países miembros pasaron a ser miembros de la UE.

sobre redes sociales en línea y el 1/2008 sobre asuntos relativos a la protección de datos vinculados a las herramientas de búsqueda, los cuales tienen por finalidad adecuar la interpretación de normativa de la Directiva 46/95/CE en el ámbito de internet.

Para otorgar eficiencia a las directrices y normas mencionadas, la UE y el Consejo de Europa consideraron que para asegurar el cumplimiento de estas disposiciones era esencial crear una autoridad de control autónoma e independiente, la cual estuviera encargada de velar por el control, la consulta y cooperación en materia de privacidad y protección de datos entre los estados comunitarios.

Como consecuencia de lo anterior, surgió el reglamento 45/2001/CE, el cual creó la figura del Supervisor Europeo de Protección de Datos, entidad encargada de garantizar y fiscalizar que las instituciones y órganos miembros de la UE respeten el derecho fundamental a la protección de datos de carácter personal. De lo anterior se puede desprender que en España existe un doble control administrativo en materia de privacidad y datos personales, es decir, por una parte tenemos el control comunitario a

cargo del Supervisor Europeo de Protección de Datos y, por otra, el control interno a cargo de la Agencia Española de Protección de Datos.

La complementariedad normativa del ordenamiento jurídico interno de España con el ordenamiento jurídico comunitario en virtud de lo dispuesto en el artículo 96 de la CE, ha tenido como consecuencia considerar a España como uno de los países a nivel internacional, con una labor legislativa, doctrinaria y jurisprudencial más completa y fecunda en materia de privacidad y protección de datos personales.

Las diversas directivas y tratados internacionales tuvieron un importante impacto en la cultura y normativa española; siendo el ejemplo fundamental la dictación de la Ley Orgánica 15/1999 sobre protección de datos personales que será tratada en el correspondiente apartado, la cual fue dictada con la finalidad de cumplir con el mandato contenido en el artículo 32.1[136] de la Directiva 95/46 del Parlamento Europeo, el cual exigía a todos sus Estados miembros que adecuaran su normativa interna en concordancia con los principales lineamientos en materia de protección de datos de carácter personal, contenidos en la referida directiva.

[136] Otorgaba a los estados miembros un plazo de 3 años desde la adopción de la misma para que adoptasen las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en ella.

3. Constitución española.

La actual Constitución española[137] (en adelante, "CE", indistintamente) fue promulgada en el año 1978, marcando con este acontecimiento la culminación de la transición a la democracia. En este contexto surge la redacción del artículo 18 de la CE, el cual fue una novedad en la época de su dictación, por motivo de proteger en una sola norma varios derechos de múltiples contenidos, al disponer lo siguiente:

"Artículo 18:

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

[137] La Constitución de España al igual que la Constitución chilena ha seguido la tradición francesa al estructurar su articulado en una parte dogmática, al tratar los principios constitucionales y derechos fundamentales y, por otra, una parte orgánica, la que hace referencia a la división de poderes y la organización política y territorial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Se estima por parte de la doctrina[138] que estos derechos, si bien son autónomos entre sí, pretenden proteger una serie de bienes jurídicos lo suficientemente semejantes como para que puedan ser conculcados por medios análogos por parte de los particulares; en efecto, la transgresión a cualquiera de estos derechos se traduce en el detrimento de la dignidad del ser humano, principio reconocido en el artículo 10 de la CE.

España a diferencia de Chile, se ha encargado de regular a través de la dictación de diversas leyes sectoriales los derechos reconocidos en el artículo 18 de la CE; pues, como hemos dicho con anterioridad, no basta con el reconocimiento expreso de los derechos, si no se establecen verdaderos mecanismos que aseguren su protección y su cumplimiento.

[138] PARDO, Javier. 1992. Los derechos del artículo 18 de la Constitución española en la jurisprudencia del Tribunal Constitucional. Revista Española de Derecho Constitucional 12(34).

En concordancia con lo anterior, es importante destacar dos leyes sectoriales que, desde el ámbito civil, protegen y aseguran el cumplimiento de los derechos reconocidos en el artículo 18 de la CE; referidos a la Ley Orgánica 1/1982, la cual se encarga de estructurar una serie de disposiciones tendientes a proteger los derechos reconocidos en el artículo 18.1 de la CE, es decir el derecho al honor, a la intimidad personal y familiar, y propia imagen; y, a la Ley 15/1999 destinada a cautelar al derecho a la autodeterminación informativa, garantía contenida en el artículo 18.4 de la CE. Cabe señalar que es de vital importancia la dictación de estas leyes, ya que España al igual que Chile tiene un sistema jurídico basado en el derecho continental, siendo por tanto la ley el principal eje rector en la interpretación y aplicación de estos derechos.

Asimismo, el constituyente también ha establecido un mecanismo de protección a nivel constitucional para los derechos reconocidos en el artículo 18 de la CE, me refiero al recurso de amparo, el cual exige, para su interposición ante el Tribunal Constitucional Español (en adelante, "TCE", indistintamente), el agotamiento de todas las instancias en la vía judicial ordinaria previa y reguladas en la correspondiente ley orgánica y, además, de haber invocado la transgresión de alguna de estas garantías, tan pronto

como fuera posible acudir ante el Tribunal Constitucional Español, lo cual es claramente más eficiente y efectivo, en contraste con la realidad de Chile, que ha sido criticado en el apartado anterior.

A mayor abundamiento, España, debido a este *modus operandi*, cuenta con jueces más interiorizados en el conocimiento del caso en concreto, ya que lo ideal es que el conflicto se solucione en primera instancia y, además, descongestiona el sistema judicial del Tribunal Constitucional Español.

Se debe señalar que los derechos reconocidos en el artículo 18 de la CE no son absolutos, ya que pueden ser limitados por el ejercicio de otros derechos fundamentales cuando se cumplen ciertas condiciones en el ordenamiento jurídico, escenario en el cual la jurisprudencia es la que en cada caso en concreto analiza qué derecho prevalece sobre otro, siendo de vital trascendencia las sentencias dictadas por el TCE a este respecto, ya que promueven la unificación de criterios y el desarrollo conceptual de los derechos contenidos en el artículo 18 de la CE.

A continuación, se describirá el derecho a la intimidad, propia imagen e inviolabilidad del domicilio y comunicaciones secretas, desde la perspectiva del Tribunal Constitucional Español, ya que al igual que en el caso de

nuestro país, el legislador español ha encargado el establecimiento del contenido y alcance de estos derechos a la jurisprudencia.

3.1. Derecho a la intimidad.

En Europa, por regla general, la configuración del derecho a la intimidad se ha introducido por vía de interpretación constitucional, siendo por tant, España una excepción, por motivos de reconocer explícitamente este derecho en el artículo 18.1 de la CE. Como señala el Tribunal Constitucional Español, lo anterior se fundamenta debido a que "el avance de la tecnología actual y el desarrollo de los medios de comunicación en masas han obligado extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De ahí que el reconocimiento global de un derecho a la intimidad o vida privada que abarque las intromisiones que, por cualquier medio, puedan realizarse en ese ámbito reservado de la vida"[139].

[139] ESPAÑA. Tribunal Constitucional. Sentencia 110/1994.

En efecto, con anterioridad a la Constitución de 1978 se protegía la inviolabilidad del domicilio y del respeto a la correspondencia, desde una perspectiva negativa y restringida al ámbito tangible. Posteriormente, durante la tramitación de la Constitución de 1978, el legislador intuyó la necesidad e importancia de reconocer el derecho genérico a la intimidad de forma expresa, con la finalidad de poder enfrentar las nuevas e impensables amenazas que pudieran surgir contra la intimidad de las personas, por motivos del transcurso del tiempo y evolución que vive toda sociedad.

Es importante señalar que la doctrina mayoritaria, la cual concuerda con las principales sentencias dictadas por el Tribunal Constitucional Español, ha esgrimido que, con excepción del derecho al honor y al secreto de las comunicaciones, los demás derechos reconocidos en el artículo 18 de la CE serían manifestaciones del derecho a la intimidad[140]; sin embargo, nos referiremos a este punto más adelante al describir los demás derechos reconocidos en el artículo 18 de la CE, en forma individual.

Ahora bien, en cuanto al concepto del derecho a la intimidad, es importante mencionar que la Constitución Española y demás leyes

[140] PARDO, Javier. Los derechos del artículo 18 de la Constitución española en la jurisprudencia del Tribunal Constitucional. Óp. Cit. 158p.

relacionadas no definen el derecho a la intimidad, siendo entregada la construcción de este derecho a la jurisprudencia y el Tribunal Constitucional Español, quien es el encargado de principales contenidos y alcances de este derecho, definiendo el derecho a la intimidad como "la esfera más reservada de las personas, al ámbito que estas siempre preservan de las miradas ajenas, aquél que desea mantenerse oculto a los demás por pertenecer a su esfera más privada"[141].

Esta esfera reservada de protección protege tanto a la intimidad personal y familiar. Respecto al derecho a la intimidad familiar, el TCE ha llegado a considerar que el entorno familiar, puede ser transgredido no solo de forma directa, sino que también indirecta, debido a que la vulneración a la intimidad personal de un individuo, en ciertos casos, por reflejo, puede transgredir la intimidad de su familia[142].

En cuanto al debate terminológico de vida privada e intimidad, corresponde señalar que el ordenamiento jurídico español, no hace

[141] ESPAÑA. Tribunal Constitucional. Sentencia 151/1997.

[142] El Tribunal Constitucional Español ha señalado "Prevalecerá el derecho a la intimidad del menor adoptado, y por reflejo, el de la intimidad familiar de sus padres adoptivos en relación con otras circunstancias de la adopción no reveladas". ESPAÑA. Tribunal Constitucional. Sentencia 197/1991. 90p.

diferencia conceptual, siendo considerado a nivel normativo como términos intercambiables, a pesar que no lo son, como se analizó en el primer capítulo de esta tesis y en la historia de la ley del artículo 19 N° 4 de la Constitución Política de la República de Chile, en el segundo capítulo.

Es del caso señalar, que España, por motivo de su desarrollo normativo, doctrinal y sobre todo jurisprudencial, ha tenido oportunidad de asentar, por medio de la labor de su Tribunal Constitucional, los principales elementos a considerar, para determinar en cada caso particular, cuando se transgrede de forma ilegítima el derecho a la intimidad y, en consecuencia, se pueda establecer la preeminencia de este derecho, sobre otros; siendo la principal colisión de derechos, entre el de la intimidad y el de la libertad de expresión.

En este sentido, el Tribunal Constitucional ha señalado que no toda intromisión a la intimidad, implica una vulneración a la garantía fundamental reconocida en el artículo 18. Por tanto, para que dicha intromisión importe una transgresión al derecho a la intimidad, se deben analizar los siguientes elementos:

- Ilegitimidad en la intromisión: en efecto, no se considerará ilegítima la intromisión a la intimidad, en todos aquellos casos, en que dicha transgresión es autorizada por el ordenamiento jurídico cesa en función del interés público[143].

- Veracidad del hecho: el Tribunal Constitucional considera la veracidad como presupuesto necesario para que la intromisión a la privacidad se pueda considerar legitima en función del interés público, pues por lógica los hechos de interés público son los verdaderos[144].

- Condición de figura pública o privada de la supuesta víctima: en efecto, el Tribunal Constitucional ha señalado que las personas que son personajes públicos han de sufrir mayores intromisiones en su vida privada que los simples particulares, pero ello no puede ser entendido radicalmente en el sentido de que el personaje público acepte libremente el riesgo de lesión de la intimidad que implica la figura pública. En conclusión, la figura pública tiene derecho a la

[143] ESPAÑA. Tribunal Constitucional.1989. Registro domiciliario autorizado judicialmente. Sentencia 37/1989.
[144] ESPAÑA. Tribunal Constitucional.1991.Sentencia 197/1991.

intimidad, el cual emana de la dignidad que tiene todo ser humano, pero el grado de este derecho es menor en comparación al que tiene una figura privada.

Asimismo, el Tribunal Constitucional Español ha considerado que para apreciar estos límites, anteriormente expuestos, deberá prevalecer por regla general el derecho a la intimidad sobre el derecho a la libertad de información; otra gran diferencia con nuestro país, puesto que nuestros Tribunales de Justicia han sido cautos en cuanto al establecimiento de los principales criterios a considerar en casos de coalición de derechos[145].

3.2 Derecho a la propia imagen.

En discrepancia con la opinión de esta investigación, el Tribunal Constitucional español considera el derecho a la propia imagen, como una manifestación del derecho a la intimidad y lo define como "aquel derecho que salvaguarda la proyección exterior de dicha imagen como medio de evitar injerencias no deseadas"[146].

[145] NOGUEIRA, Humberto. Dignidad de la persona, derechos fundamentales y bloque constitucional de derechos: una aproximación desde Chile y América Latina. Óp. Cit. pp. 79-142.
[146] ESPAÑA. Tribunal Constitucional. 2001. Sentencia 139/2001.

De lo anterior se coligen dos características importante de este derecho, por una parte el TCE considera este derecho como una concreción desde el ámbito tangible del derecho a la intimidad, por cuanto protege la voz[147] y la imagen, y, por otra, parte sería una manifestación desde la perspectiva positiva del derecho a la intimidad, en cuanto el Tribunal Constitucional señala que lo que se pretende proteger con el reconocimiento explícito de este derecho es la libre determinación de los individuos, en cuanto les otorga el derecho a decidir qué aspectos de su persona desean preservar de la difusión pública, a fin de garantizar un ámbito privado para el desarrollo de la propia personalidad ajeno a injerencias externas[148].

Como es de observar, el derecho a la propia imagen, al tener reconocimiento explícito a nivel constitucional y en la Ley Orgánica 1/1985, ha permitido a los tribunales que puedan desarrollar a nivel jurisprudencial sus principales alcances y límites; lo que permite que ante la evolución de los medios tecnológicos y de comunicación, medios que

[147] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online.[en línea] <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf]> [consulta: 17 de noviembre 2015]
[148] Ibíd.43p.

generan nuevas y mayores amenazas al derecho a la propia imagen; los tribunales puedan adaptar la normativa existente a cada caso en concreto y, desarrollar criterios generales.

Dentro de este contexto, el TCE estima que para analizar si en un determinado caso se configura la transgresión del derecho a la propia imagen, es necesario considerar la actividad profesional, laboral o la relevancia pública de la persona que alega la vulneración de este derecho. Si bien dicho elemento también es considerado en un supuesto caso de transgresión del derecho genérico a la intimidad, en el derecho a la propia imagen es aún más importante, por cuanto el riesgo de vulneración a este derecho aumenta por el indebido y arbitrario uso que los medios de comunicación social puedan hacer de la imagen, voz y nombre de una persona, justificando su actor en la calidad de figura pública de una determinada persona[149].

[149] Ibíd. 43p.

3.3. Derecho a la inviolabilidad del domicilio.

Si bien esta tesis no se centra respecto a este punto, se mencionarán los principales aspectos generales de este derecho reconocido en el artículo 18.2 de la CE, al ser considerado una proyección del derecho a la intimidad.

Al respecto, el Tribunal Constitucional ha señalado que el domicilio es el espacio en el cual el individuo vive sin estar sujeto necesariamente a los usos y convenciones sociales y además, ejerce su libertad más íntima[150].

Por individuo se debe entender a toda persona natural y, además, a diferencia de nuestro país, otorga protección también a las personas jurídicas, sin perjuicio que exista debate respecto al fundamento constitucional de dicha protección[151] y, en cuanto a considerarlo como una manifestación de su libertad más íntima, tiene esto como consecuencia que no solo se protege el espacio físico en sí, sino lo que en él hay de emanación de la persona y su esfera privada.[152] Es decir, se protege de cualquier perturbación que sufra una persona en su domicilio. Es más, la Agencia Española de Protección de Datos ha señalado que esta

[150] ESPAÑA. Tribunal Constitucional. 1983. Sentencia 22/1984.
[151] Porque el derecho a la intimidad emana de la dignidad de todo ser humano en consecuencia, las personas jurídicas no pueden tener derechos personalísimos pues no tienen dignidad.
[152] ESPAÑA. Tribunal Constitucional. 1984. Sentencia 22/1984.

interpretación amplia permite proteger de toda intromisión que puede sufrir una persona por motivos del uso de nuevas tecnologías, tales como webcam, captación de fotos y videos, entre otros[153].

3.4. Derecho al secreto de las comunicaciones.

El derecho al secreto de las comunicaciones se encuentra reconocido en el artículo 18.3 de la CE. Es menester señalar que en este derecho encuentra una de las diferencias más radicales en comparación con la experiencia de nuestro país. En efecto, en Chile el derecho a la inviolabilidad de las comunicaciones privadas ha llegado a ser considerado por parte de la doctrina mayoritaria como una proyección del derecho a la vida privada; mientras que en España, el Tribunal Constitucional Español ha señalado que el derecho al secreto de las comunicaciones es un derecho autónomo e independiente respecto al derecho a la intimidad pues como bien señala la Agencia Española de Protección de Datos "las comunicaciones deberán

[153] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online.[en línea] <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf]> [consulta: 17 de noviembre 2015]

resultar protegidas con independencia de su contenido, esto es, ya se trate de comunicaciones de carácter íntimo o de otro género"[154].

Señal de lo anteriormente expuesto, consiste en la simple referencia que hace el artículo 18.3 al establecer como derecho fundamental el secreto de las comunicaciones, sin señalar el carácter de privado como ocurre en el caso de Chile.

De esta forma lo que en España se protege es la libertad de las comunicaciones, es decir, protege la libertad de elegir a los destinatarios de nuestras comunicaciones.[155] De lo anterior, se colige que este derecho protege tanto la comunicación como su contenido; concretándose su transgresión tanto por la interceptación en sentido material[156] o captación por intermedio de otro medio de comunicación, como por ejemplo el internet o el ya conocido *inbox* de Facebook.

Sin perjuicio de haberse señalado que este derecho en España es independiente y autónomo al derecho a la intimidad; existen ciertas

[154] Ibíd.77p.
[155] FALCÓN, Javier. 1992. Los derechos del artículo 18 de la Constitución española en la jurisprudencia del Tribunal Constitucional. Revista Española de Derecho Constitucional 12(34).
[156] Aprehensión física de un escrito.

situaciones respecto a las cuales puede existir incertidumbre en relación al derecho vulnerado. Para conciliar este punto, el TCE ha establecido como principal criterio rector para el esclarecimiento de esta situación la presencia de un elemento ajeno a aquellos entre los que media el proceso de comunicación. Por tanto, se considera indispensable la presencia de este elemento, para configurar el ilícito constitucional del precepto. En efecto, si uno de los intervinientes es quien revela la comunicación, no se configurará la transgresión del derecho al secreto de las comunicaciones, sino que estaríamos en presencia de un caso de vulneración al derecho a la intimidad del otro interviniente[157].

En directa relación con lo anteriormente expuesto, respecto al uso de las nuevas tecnologías, la Agencia Española de Protección de Datos ha señalado que "el secreto de las comunicaciones se proyectará sobre todos aquellos servicios de las redes sociales que comporten una comunicación interpersonal que excluya a terceros distintos de los intervinientes"[158]. En síntesis, en las redes sociales también se ha de aplicar el criterio

[157] ESPAÑA. Tribunal Constitucional. 1984. Sentencia 114/1984.
[158] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. Óp. Cit. 77p.

anteriormente expuesto por el TCE respecto al elemento ajeno, para así establecer si existiría una vulneración al secreto de las comunicaciones o a la intimidad, pues la doctrina jurisprudencial española, otorga tutela frente a interferencias en todo tipo de comunicaciones "cualquiera sea la técnica de transmisión utilizada y con independencia del contenido del mensaje, conversaciones, datos, imágenes, etc."[159].

En Chile, el tema del secreto de las comunicaciones desde la perspectiva tecnológica ha sido zanjado, en parte, desde el ámbito jurisprudencial, ya que solo ha existido un pronunciamiento trascendental respecto a los correos electrónicos, sin existir hasta la fecha, un mayor pronunciamiento respecto al caso de las redes sociales, pues el límite entre lo público y privado es más difuso de establecer.

3.5. Derecho a la protección de datos de carácter personal.

A diferencia de los demás apartados del artículo 18 de la Constitución Española, el derecho a la protección de datos de carácter personal no está reconocido de forma literal en el artículo 18.4[160], debido a que la

[159] Ibíd. 77p.
[160] La ley limitará el uso de la informática.

construcción de este derecho es de una época posterior, siendo desarrollado en gran parte por la doctrina y jurisprudencia.

La consagración a nivel de garantía constitucional del derecho a la protección de datos de carácter personal se colige de una interpretación en conjunto del artículo 18.4 el cual dispone: "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos", y de lo dispuesto en el Convenio 108 del Consejo de Europa, que, como debemos recordar, en concordancia con el artículo 10.2 de la CE, sus disposiciones son parte integrante de la normativa interna española[161]. Siendo esta interpretación conjunta de vital trascendencia para asentar la primera jurisprudencia[162] por parte del Tribunal Constitucional Español respecto a este derecho de reciente configuración.

En la época de la dictación de la Constitución Española, el constituyente fue considerado un visionario, pues en esos años los peligros de la

[161] Siendo este el motivo por el cual España decidió acoger la denominación de derecho a la protección de datos de carácter personal debido a que permite identificar de forma concreta el contenido de protección de dicho derecho, particularmente el bien jurídico que se pretende proteger y la técnica empleada.

[162] MURILLO DE LA CUEVA, Pablo. 1999. La construcción del derecho a la autodeterminación informativa. Revista de Estudios Políticos 104:35-60.

informática eran impensables y escasos. Sin embargo, en el ordenamiento jurídico español ya existía una preocupación hacia el futuro por el vertiginoso progreso que pudiesen alcanzar las tecnologías; motivo por el cual el constituyente decidió limitar el uso de la informática a nivel constitucional[163].

Es importante señalar que la redacción del artículo 18.4 de la CE no estuvo exento de debate en el anteproyecto constitucional, pues se discutía si era necesaria la consagración explicita de este derecho contenido 18.4 de la CE.

Los que estaban en contra de su consagración explícita señalaban que la redacción de dicho enunciado sería redundante e ineficiente. Sería redundante al estimar que el derecho al honor y a la intimidad consagrados en el artículo 18.1 de la CE ya protegían a las personas contra el uso indiscriminado de la informática; y sería ineficiente, por motivo de

[163] Con la finalidad de modernizar la justicia y los ministerios en España surgieron una serie de medidas tendientes a estudiar y buscar finalidad los derechos de las personas frente a las amenazas de la informática, para tales efectos, se dictó una orden ministerial de justicia de 18 de febrero de 1970 convocadas "jornadas de estudio y perfeccionamiento y modernización de los medios y métodos de justicia". Además, ese mismo año se promulgó un decreto presidencial del gobierno por el que expresamente se creó una comisión interministerial de informática y un servicio central de informática cuya misión es supervisar y apoyar el esfuerzo de programación informática de los distintos ministerios.

considerar inoportuno hacer mención expresa a la informática y no a otra serie de técnicas o medios que también pueden transgredir la intimidad y honor de los ciudadanos[164], por tanto se caería en una suerte de positivismo en exceso. Sin embargo, esta postura no prosperó, siendo aceptada en consecuencia la consagración explicita de este derecho.

El motivo esencial para aceptar la consagración explícita de este derecho, residió en considerar que el uso de la informática no solo ha interferido en el ejercicio del derecho al honor o a la intimidad, sino que también de otros derechos fundamentales. Por tanto, deducir su reconocimiento implícito desde el artículo 18.1 de la CE, implicaba dejar desprotegidos a los demás derechos fundamentales, contra los usos de la informática. En síntesis, el constituyente decidió otorgar un sentido amplio de protección frente a los posibles abusos de la informática[165].

A nivel de leyes sectoriales, al igual que con los derechos anteriormente descritos del artículo 18 de la CE, el constituyente otorgó un mandato expreso en el artículo 18.4 de la CE, destinado a la creación de una ley

[164] PÉREZ LUÑO, Antonio. 1981. Informática y libertad. Comentario al artículo 18.4 de la Constitución Española. Revista de Estudios Políticos (24):31-53.
[j]Ibíd. 12p.

sectorial que se encargara de estructurar, regular y limitar los usos de la informática. Se materializa este mandato en la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal y la actual normativa vigente contenida en la Ley Orgánica 15/1999 de protección de datos de carácter personal. Dichas disposiciones, que están en directa relación con lo estipulado en el artículo 18.4 de la CE, han permitido al Tribunal Constitucional Español desarrollar el contenido esencial del artículo 18.4 de la CE, llegando a las siguientes conclusiones:

- El contenido del derecho fundamental a la protección de datos se manifiesta jurídicamente en la facultad de consentir la recogida, obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular.

- Para que el titular de los datos de carácter personal, pueda ejercer este derecho, se le debe reconocer la facultad de saber en todo momento quien dispone de esos datos personales y a que uso los están sometiendo, y, por otro lado, el poder para oponerse al tratamiento de

dichos datos. Siendo esta la faceta positiva del derecho a la protección de datos personales.

- El derecho a la protección de datos comprende la protección de todo tipo de datos de carácter personal, sean íntimos, públicos o de otra índole.

De lo anterior, se colige que el Tribunal Constitucional Español otorgó una interpretación amplia del artículo 18.4 de la CE, por motivos de reconocer dentro de su esfera el amparo no solo los datos de carácter personal de índole privada, sino que también los de otra especie e incluso los públicos.

Respecto a los datos personales de carácter público el Tribunal Constitucional Español estimó que estos derechos son dignos de protección por parte del artículo 18.4 de la CE, en razón de que no por ser datos accesibles al conocimiento de cualquiera el afectado deba ver mermado su poder de disposición de los datos que le conciernen directamente a él, y por tanto, protegidos por el derecho a la protección de datos de carácter

personal[166]. Siendo este uno de los principales motivos por el cual en España a nivel jurisprudencial no existe discusión respecto a la naturaleza jurídica de este derecho, reconociéndose en tal forma su rango de garantía constitucional, autonomía e independencia respecto al derecho a la intimidad; lo cual, si bien es contrario al postulado de esta tesis, es necesario reconocer el beneficio que conlleva esta autonomía, pues permite identificar y dilucidar de mejor forma el hecho que configura la transgresión de la garantía a nivel constitucional. Pues el derecho a la protección de datos de carácter personal es considerado en España un derecho fundamental autónomo destinado a controlar el flujo de informaciones que conciernen a cada persona[167].

Además, el Tribunal Constitucional consideró en la construcción de este derecho la perspectiva negativa y positiva de esta garantía. La configuración negativa del derecho a la protección de datos de carácter personal se traduce en el derecho a no hacer de dominio público ciertas informaciones de carácter personal, privado o reservado; mientras que la

[166] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. Óp. Cit. 93p.
[167] MURILLO DE LA CUEVA, Pablo. La construcción del derecho a la autodeterminación informativa. Óp. Cit.13p.

perspectiva positiva implica otorgar a su titular un derecho al control de los datos concernientes a la propia persona[168].

Para finalizar, se debe señalar que el derecho a la protección de datos de carácter personal es el derecho que mayores transgresiones ha sufrido en el ámbito de internet y en específico en las redes sociales. Por tanto la labor del Tribunal Constitucional Español es de trascendental importancia en cuanto debe interpretar las normas contenidas a nivel constitucional y ley sectorial, en concordancia con la época y cultura actual; para que de esta forma pueda otorgar una eficaz protección los derechos y libertades de los ciudadanos, frente a los peligros actuales que conlleva el uso y evolución de las TIC.

4. Principales leyes orgánicas.

4.1 Ley Orgánica 1/1982.

Los derechos reconocidos en el artículo 18.1 de la Constitución Española se encuentran regulados en la Ley 1/1982 de 5 de mayo[169], de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia

[168] PÉREZ LUÑO, Antonio. Informática y libertad. Comentario al artículo 18.4 de la Constitución Española. Óp. Cit. 45p.
[169] Para consultar normativa española recomendamos [en línea] <https://www.boe.es> [consulta: 29 de noviembre de 2015]

imagen. Además, esta ley es la encargada de regular el derecho a la protección de datos personales contenido en el artículo 18.4 de la CE de forma transitoria[170] hasta la promulgación de la correspondiente normativa.

La Ley 1/1982 se estructura en dos capítulos, compuestos de tan solo 9 artículos. Esta normativa tiene por finalidad proteger los derechos reconocidos en el artículo 18.1 de la CE mediante la estructuración de un sistema de responsabilidad civil en contra de las intromisiones ilegítimas que puedan sufrir las personas vivas y fallecidas en su esfera personal.

Es importante señalar que la Ley 1/1982 no define ninguno de los derechos protegidos y regulados en ella. Lo anterior se debe a que el derecho al honor, a la intimidad y propia imagen son derechos cuyo contenido y límites de protección mutan con el transcurso del tiempo, siendo entregada a la jurisprudencia la labor de definir y por tanto fijar los alcances de esta

[170] Disposición transitoria primera: En tanto no se promulgue la normativa prevista en el artículo dieciocho, apartado cuatro, de la Constitución, la protección civil del honor y a la intimidad personal y familiar frente a las intromisiones ilegitimas derivadas del uso de la informática se regulará por la presente ley.

normativa; debiendo tener en consideración para tales efectos los usos sociales[171] de la nación.

La Ley 1/1982 reconoce de forma expresa que el derecho al honor, a la intimidad y propia imagen son garantías que emanan de la personalidad del ser humano, y en consecuencia son irrenunciables, inalienables e imprescriptibles[172]. Sin embargo, se debe señalar que estos derechos no son absolutos e ilimitados, ya que el legislador también se encargó de consagrar en forma expresa las limitaciones que pueden afectar a estos derechos, siendo para tales efectos el interés público, cuando estuviere expresamente autorizada por ley o cuando el titular del derecho hubiese otorgado al efecto su consentimiento expreso[173].

En cuanto al consentimiento del interesado, la Ley 1/1982 señala que no se no se opone a una irrenunciabilidad abstracta, pues el consentimiento no implica la absoluta abdicación de los mismos sino tan solo el parcial

[171] Artículo 2.1: "La protección civil del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia.
[172] Artículo 1.3: "El derecho al honor, a la intimidad personal y familiar y a la propia imagen es irrenunciable, inalienable e imprescriptible. La renuncia a la protección prevista en esta ley será nula, sin perjuicio de los supuestos de autorización o consentimiento a que se refiere el artículo segundo de esta ley".
[173] Artículo 2.2: "No se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por ley o cuando el titular del derecho hubiese otorgado al efecto su consentimiento expreso".

desprendimiento de alguna de las facultades que los integran. Para efectos de que el consentimiento sea válido en los términos de la ley y, por tanto, no se configure una intromisión ilegítima, este debe ser expreso y puede ser revocado en cualquier momento, pero habrán de indemnizarse en su caso los daños y perjuicios causados, incluyendo en ellos las expectativas justificadas, que de la revocación surgieran[174]. Asimismo, el legislador estableció requisitos adicionales respecto a la manifestación del consentimiento realizada por los menores de edad e incapaces[175], con la finalidad de resguardar los derechos de los individuos más vulnerables.

En los artículos 7 y 8 de la Ley 1/1982 el legislador español plasmó los criterios generales y no taxativos, que debe ser considerados por labor jurisprudencial para el establecimiento de cuando una intromisión será ilegitima y por tanto, proceden sanciones emanadas de la responsabilidad civil.

[174] Artículo 2.3: "El consentimiento a que se refiere el párrafo anterior será revocable en cualquier momento, pero habrán de indemnizarse en su caso, los daños y perjuicios causados, incluyendo en ellos las expectativas justificadas".
[175] Artículo 3: "Uno. El su representante legal, quien estará obligado a poner en conocimiento previo del Ministerio Fiscal el consentimiento proyectado. Si en el plazo de ocho días el Ministerio Fiscal se opusiere, resolverá el Juez".

Así, el artículo 7[176], en palabras del legislador, recoge en términos de razonable amplitud diversos supuestos de intromisión o injerencia que pueden darse en la vida real y coinciden con los previstos en las legislaciones protectoras existentes en otros países de desarrollo social y tecnológico. Mientras que el artículo 8[177] señala una serie de casos en que tales injerencias o intromisiones no pueden considerarse ilegítimas en virtud

[176] Artículo 7: "Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley: 1) El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas. 2) La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción. 3) La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo. 4) La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela. 5) La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo octavo, dos. 6) La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.7) La divulgación de expresiones o hechos concernientes a una persona cuando la difame o la haga desmerecer en la consideración ajena".

[177] Artículo 8: 1) No se reputará, con carácter general, intromisiones ilegítimas las actuaciones autorizadas o acordadas por la Autoridad competente de acuerdo con la ley, ni cuando predomine un interés histórico, científico o cultural relevante. Dos. En particular, el derecho a la propia imagen no impedirá: a) Su captación, reproducción o publicación por cualquier medio cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público. b) La utilización de la caricatura de dichas personas, de acuerdo con el uso social. c) La información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesoria. Las excepciones contempladas en los párrafos a) y b) no serán de aplicación respecto de las autoridades o personas que desempeñen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza.

de razones de interés público que imponen una limitación de los derechos individuales, como bien se mencionó con anterioridad.

Para finalizar, en forma de clausura y otorgando eficacia a la normativa contenida en la Ley 1/1982 y, en concordancia con el artículo 53.2 de la CE[178], el artículo 9[179] establece la posibilidad de defensa frente a las injerencias o intromisiones ilegitimas, así como las pretensiones que puede

[178] Artículo 53.2 de la CE: "Cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el artículo 14 y la Sección primera del Capítulo segundo ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional. Este último recurso será aplicable a la objeción de conciencia reconocida en el artículo 30.

[179] Artículo 9 de la CE: 1) La tutela judicial frente a las intromisiones ilegítimas en los derechos a que se refiere la presente ley podrá recabarse por las vías procesales ordinarias o por el procedimiento previsto en el artículo cincuenta y tres, dos, de la Constitución. También podrá acudirse, cuando proceda, al recurso de amparo ante el Tribunal Constitucional. 2) La tutela judicial comprenderá la adopción de todas las medidas necesarias para poner fin a la intromisión ilegítima de que se trate y restablecer al perjudicado en el pleno disfrute de sus derechos, así como para prevenir o impedir intromisiones ulteriores. Entre dichas medidas podrán incluirse las cautelares encaminadas al cese inmediato de la intromisión ilegítima, así como el reconocimiento del derecho a replicar, la difusión de la sentencia y la condena a indemnizar los perjuicios causados. 3) La existencia de perjuicio se presumirá siempre que se acredite la intromisión ilegítima. La indemnización se extenderá al daño moral que se valorará atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente producida, para lo que se tendrá en cuenta en su caso, la difusión o audiencia del medio a través del que se haya producido. También se valorará el beneficio que haya obtenido el causante de la lesión como consecuencia de la misma.4)El importe de la indemnización por el daño moral, en el caso del artículo cuarto, corresponderá a las personas a que se refiere su apartado dos y, en su defecto, a sus causahabientes, en la proporción en que la sentencia estime que han sido afectados. En los casos del artículo sexto, la indemnización se entenderá comprendida en la herencia del perjudicado. 5) Las acciones de protección frente a las intromisiones ilegítimas caducarán transcurridos cuatro años desde que el legitimado pudo ejercitarlas.

deducir el perjudicado. Como bien señala el legislador, en lo que respecta a la indemnización de perjuicios se presume que estos existen en todo caso de injerencias o intromisiones acreditadas, y comprenderán no solo la de los perjuicios materiales, sino también la de los morales, de especial relevancia en este tipo de actos ilícitos.

En virtud de estas consideraciones, se puede concluir que la Ley 1/1982 se encarga de estructurar en términos generales los principales lineamientos que deben considerar los tribunales de justicia para una correcta interpretación del artículo 18.1 de la CE. De esta forma, el legislador buscaba evita caer en la obsolescencia siendo este el motivo por el cual decidió regular esta materia en tan solo 9 artículos, con la finalidad de que dicha normativa pueda ser eficaz en contra de las nuevas amenazas que surjan contra el derecho al honor, intimidad y propia imagen.

Finalmente, se debe mencionar que el proyecto original de la Ley 19.628 de nuestro país claramente se inspiró en la ley española 1/1982; sin embargo, como bien estudiamos en el capítulo anterior, el proyecto lamentablemente no prosperó, por lo que carecemos hasta el día de hoy con

una eficaz normativa desde el ámbito civil que proteja el derecho a la vida privada.

4.2. Ley Orgánica 15/1999.

Antes de entrar en detalle respecto a la normativa vigente en España referente a la protección de datos personales es menester hacer mención a su antecesora y considerada la primera ley orgánica sobre protección de datos en España. Se trata de la Ley Orgánica 5/1992 de 29 de octubre "Sobre regulación del tratamiento automatizado de los datos de carácter personal" (en adelante, "LORTAD", indistintamente), la cual estuvo en vigencia hasta el 14 de enero del año 2000.

De la LORTAD es posible destacar su exposición de motivos, pues la ley 15/1999 carece de este apartado, estimando en consecuencia la doctrina que estos motivos también deben ser considerados en la normativa vigente.

La referida exposición destaca por realizar por primera y única vez a nivel normativo en España, la diferenciación conceptual entre privacidad e intimidad. De esta forma señala que la privacidad es más amplia que esta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona, la privacidad

constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que coherentemente enlazadas entre sí arrojan como precipitado un retrato de la personalidad del individuo que este tiene derecho a mantener reservado. Lo anterior corresponde al fundamento respecto al cual se desprende la estrecha relación entre privacidad y protección de datos personales, sin perjuicio que a nivel constitucional y jurisprudencial se han consolidado como derechos autónomos e independientes. Además, en dicha normativa se hace mención por vez primera a la creación de una Agencia de Protección de Datos[180].

Ahora, por motivo de la transposición de la normativa contenida en la Directiva 95/46/CE a la realidad española, surgió la imperiosa necesidad para el legislador de adoptar un nuevo texto de protección de datos personales; en vez de reformar la LORTAD, estimó que dado el estado actual de la tecnología dicha normativa estaba obsoleta, siendo necesario crear un cuerpo normativo desde cero[181].

[180] En el artículo 34 de la Ley Orgánica 5/1992 se hablaba de Agencia de Protección de Datos.
[181] CAMPUZANO, Herminia. Vida privada y datos personales: su protección jurídica frente a la sociedad de la información. Óp. Cit. 91p.

En consecuencia de lo anterior, surge la ley 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD); normativa encargada de cumplir con el mandato establecido en el artículo 18.4 de la CE, el cual se traduce en otorgar una efectiva protección a los datos de carácter personal frente a los diversos usos informáticos de los que se pueden valer tanto particulares como entes públicos en la recogida y tratamiento de dichos datos. Asimismo, con la finalidad de otorgar eficacia y eficiencia al sistema normativo otorga en su articulado una serie de facultades y funciones a la Agencia Española de Protección de Datos, entidad que será tratada en detalle en el capítulo siguiente.

La Ley Orgánica 15/1999, en la época de su dictación, entregó al gobierno el mandato de reglamentar una serie de procesos y potestades no definidas en la referida ley, los cuales se materializaron por la dictación del Real Decreto 1720/2007 de 21 de diciembre, Reglamento de Ley de Protección de Datos (en adelante, RDLOPD), normativa que debe ser interpretada y complementada con las disposiciones contenidas en la LOPD.

A continuación, se procede a describir y analizar las principales disposiciones en materia de protección de datos contenidas tanto en la LOPD y RDLPOD, las cuales están en directa concordancia con lo consagrado en la Directiva 95/46/CE.

i) Disposiciones generales.

El artículo 1° de la LOPD señala que el objeto de protección de esta ley es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. Es de destacar que este artículo no solo protege y garantiza el aspecto negativo del derecho a la protección de datos personales en cuanto a ser un límite para el uso de la informática, sino que además reconoce a la informática como un medio de incremento de progreso social, por tanto garantiza la libertad informática en la medida en que se respete y protejan los derechos establecidos en esta ley[182].

Las disposiciones de la LOPD y RDLOPD se aplicarán a todos los datos de carácter personal registrado en soporte físico y, a toda modalidad de uso

[182] DELGADO, L. y SALTOR, C. 2014. El derecho a la protección de datos en España y Argentina: orígenes y regulación vigente. España, Editorial Dykinson. 65p.

posterior de estos datos por los sectores públicos o privados. En conclusión, el legislador busca proteger todos los datos personales que consten en ficheros físicos y automatizados.

Como en toda normativa existente en protección de datos personales, al ser un área del derecho en el cual es necesario manejar una serie de tecnicismos y conceptos, el legislador en el artículo 3 establece una serie de definiciones. Es importante mencionar que tanto nuestra normativa actual contenida en la Ley 19.628 como la reforma en tramitación adquirieron de la normativa española, y en específico de la Directiva 95/46/CE, ciertas definiciones al mismo tenor y esencia, tales como dato de carácter personal, procedimiento de disociaciones, entre otras; existiendo mínimos cambios formales pero que, sin embargo, mantienen la esencia de las definiciones que comparten ambas naciones, siendo este el motivo por el cual no se entrará en detalle respecto a las principales definiciones, pues ya fueron analizadas al estudiar la realidad de Chile.

Pese a lo anterior, cabe mencionar que si bien tanto España como Chile recogen en los mismos términos las mismas definiciones técnicas, los alcances de protección e interpretación en España constan de una mayor

elaboración, en virtud de la labor en conjunta realizada por sus Tribunales de Justicia, y en específico el Tribunal Constitucional y, a nivel administrativo por la Agencia Española de Protección de Datos; destacando el trabajo de esta última entidad, pues a nivel de normativa comunitaria en la actualidad se encuentra colaborando en la concepción de una nueva definición de dato de carácter personal.

ii) Principios.

En apartados anteriores, ya se ha analizado lo referente a principios generales de la protección de datos, así como los que reconocerá de forma explícita Chile en su reforma; por tanto, a continuación se procederá a analizar a grandes rasgos como son tratados en la normativa española, pues estos principios también inspiran la labor de la Agencia Española de Protección de Datos en su actuar.

En contraste con nuestra normativa vigente contenida en la Ley 19.628, la normativa española expresada en la LOPD reconoce de forma explícita los principios de información, calidad, finalidad, consentimiento y seguridad, siendo complementados en su contenido por el RDLOPD. Lo anterior permite otorgar a los responsables de los ficheros y a los titulares

de los datos personales un mayor entendimiento respecto a las principales directrices que deben considerar en su actuar en materia de protección de datos personales, siendo este uno de los motivos, por lo cual la OCDE recomienda consagrar explícitamente estos principios y esperemos se concrete su consagración explicita en la actual reforma en tramitación en Chile.

- Principio de información.

El cual está reconocido en el artículo 5° de la LOPD, artículo 18 y 19 de la RDLOPD y artículo 10 y 11 de la Directiva 95/46/CE. Dicho principio establece que en la recogida de los datos personales, se deberá informar al interesado de modo expreso, preciso e inequívoco de una serie de circunstancias, tales como la finalidad de la recogida de datos y quienes serán los destinatarios de esta información, de la consecuencia de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, de la identidad o dirección del responsable del tratamiento, o en su caso de su representante informar del caso en que el responsable del tratamiento no este establecido en el territorio de la Unión Europea y utilice en el

tratamiento medios situados en el territorio español. En concordancia con lo anterior, la Directiva 95/46/CE establece que un tratamiento leal de datos es aquel en el cual los interesados deben estar en condiciones de conocer la existencia de los tratamientos y cuando los datos se obtengan de ellos mismos contar con una información precisa y completa respecto a las circunstancias de dicha obtención. En síntesis, los titulares de los datos de carácter personal deben conocer para qué se utilizan sus datos, deben conocer la existencia de un fichero o tratamiento de sus datos y se debe indicar el responsable del fichero y su dirección o la de su representante.

- Principio de finalidad y calidad de los datos.

Es menester señalar que el legislador español ha consagrado estos dos principios en un mismo articulado, por motivos de estar en directa relación. En efecto, no basta con que los datos cumplan con los estándares o calidad exigidos por la normativa legal, pues si no cumplen con una finalidad en específica, no podrán ser recolectados ni tratados.

El contenido de estos principios se desprende del artículo 4° de la LOPD, artículo 8 y 9 de la RDLOPD y artículo 4° de la Directiva 95/46/CE. De estas normas se infieren las siguientes características:

Los datos deben recogerse con fines determinados, explícitos y legítimos, por tanto se prohíbe su utilización para otros fines. Además, deben ser adecuados, pertinentes y no excesivos[183]. También deben ser exactos y responder con veracidad a la situación de su titular, es decir se deben mantener actualizados[184].

Para finalizar, la normativa española exige que solo deben conservarse durante el tiempo necesario en concordancia con la finalidades del tratamiento, por tanto careciendo de finalidad, otorgan a su titular el derecho de oposición.

- Principio del consentimiento.

Es considerado el principio rector y de mayor trascendencia en toda normativa dedicada a la protección de los datos personales. En efecto, la concurrencia de voluntades entre el titular de datos y el responsable del tratamiento determina el inicio de una relación jurídica regida por la normativa contenida en la LOPD, RDLOPD y la autonomía de la voluntad de las partes. Este principio se desprende de lo estipulado en el artículo 6, 7

[183] Denominado en Chile como principio de proporcionalidad en la actual reforma a la Ley 19.628.
[184] La reforma chilena a la Ley 19.628 señala en su artículo 3.b que los datos deben ser exactos completos y actuales, en relación con el propósito para el cual serán utilizados.

y 11 de la LOPD, artículo 12 y 17 de la RDLOPD y artículo 17 de la Directiva 95/46/CE.

La LOPD define el consentimiento del afectado como toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen. Además, como regla general, es posible afirmar que todo tratamiento de datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo disposición en contrario de la ley.

El consentimiento será libre cuando esté exento de vicios y, será inequívoco cuando se infiera de una acción, como el consentimiento expreso, o de una omisión, como el consentimiento tácito. Además, será específico cuando el tratamiento tenga una finalidad determinada, explícita y legítima y para finalizar debe ser informado.

Respecto a la forma de obtener este consentimiento, la normativa española reconoce el consentimiento expreso y el tácito. Este último se produce cuando el afectado estando en conocimiento del tratamiento de sus datos guarda silencio y no se manifiesta en forma contraria. Muy distinto de lo estipulado en nuestra Ley 19.628, pues como se ha descrito en el

apartado anterior, por regla general el consentimiento se deberá entregar de forma expresa y por escrito, no teniendo lugar la aplicación del consentimiento tácito.

La LOPD, además, estableció una serie de casos en los cuales se exige la manifestación expresa de voluntad, como por ejemplo el tratamiento de datos sensibles, que son aquellos datos referentes a ideología, religión, creencia, etc.; teniendo como requisito extra que el interesado debe otorgar su consentimiento por escrito. Lo anterior en concordancia con lo estipulado en el artículo 16 de la CE, respecto a que nadie puede ser obligado a declarar sobre estos datos. Es importante mencionar que la reforma chilena actualmente en tramitación, pretende regular el consentimiento de los datos sensibles al mismo tenor que la actual normativa española.

Asimismo, la normativa también establece excepciones, respecto a los cuales no es necesario el consentimiento, siendo, en resumen, tres motivos: interés público, relaciones contractuales y datos que figuren en fuentes accesibles al público.

Además, el RDLOPD introduce en esta materia una importante disposición en resguardo de los sectores más vulnerables, al disponer que para tratar datos personales de menores de 14 años, es necesario contar con el consentimiento de los padres o tutores. Asimismo, señala la normativa que los datos deben ser recabados utilizando un lenguaje sencillo y fácilmente comprensivo para el menor.

De esta forma, es posible ver que España se ha preocupado de regular de forma metódica el consentimiento de los titulares de los datos personales, destacando la protección adicional que otorga a los menores de edad. En Chile nuestra actual normativa consagra el principio del consentimiento en términos generales, sin embargo nuestra reforma busca armonizar nuestra legislación con la de España, al buscar reconocer el consentimiento previo, así como establecer requisitos adicionales respecto al consentimiento de los menores de edad.

- Principio de seguridad.

Como señala la Agencia Española de Protección de Datos[185], la aplicación de medidas de seguridad se ordena a garantizar la confidencialidad, integridad y disponibilidad de los datos. La seguridad constituye un instrumento esencial para garantizar el derecho fundamental a la protección de datos.

El principio de seguridad de datos se encuentra estipulado en el artículo 9° de la LOPD, artículo 79 y siguientes. de RDLPOD y artículos 16 y 17 de la Directiva 95/46/CE. Este principio impone al responsable del fichero adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Por tanto, la normativa española estima que no se registrarán datos de carácter personal en ficheros que no reúnan con las condiciones que se determinen tanto en la LOPD y RDLOPD en relación a su integridad y seguridad.

[185] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. Óp. Cit. 36p.

Es necesario destacar que el RDLOPD viene en reglamentar los diferentes niveles de seguridad[186] que deben cumplir los diversos ficheros. Para estos efectos la ley dispone de tres niveles, (básico, medio y alto), los cuales son acumulativos. Como bien señala la Agencia Española de Protección de Datos, "las medidas de seguridad de nivel básico son exigibles en todos los casos. Las medidas de nivel medio complementan a las anteriores en el caso de ficheros clasificados en este nivel, y las de nivel alto, cuando deban adoptarse, incluyen también las de nivel básico y medio"[187]. A modo de ejemplo, el reglamento establece que los datos sensibles deberán tener un nivel alto de seguridad. Así el nivel alto de seguridad, dentro de las medidas que exige, es la conservación de dichos datos por un periodo máximo de dos años, además de cumplir con el sistema de etiquetado confidencial en el caso de los ficheros automatizados.

Para finalizar, se debe mencionar que nuestra actual normativa reconocida en la ley 19.628, no cuenta con este sistema; sin embargo la

[186] ESPAÑA. RDLOPD. artículo 81.
[187] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía de Seguridad de Datos. [en línea] <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf> [consulta: 29 de noviembre 2015]

reforma pretende incorporar el establecimiento de estas medidas de seguridad, encargando al Ministerio de Económica, Fomento y Turismo la tarea de implementar el reglamento tendiente a regular este tema, lo que será un gran avance en materia de seguridad y protección de datos.

iii) Derechos de los titulares.

Existen una serie de derechos reconocidos de forma implícita en la normativa española concernientes a la protección de datos, sin embargo, en el siguiente apartado solo se hará referencia al derecho de acceso, rectificación, cancelación y oposición, o también denominados derechos arco, los cuales se encuentran igualmente reconocidos de forma explícita en nuestro ordenamiento jurídico pero de forma general, por lo que la reforma en tramitación pretende seguir el ejemplo de España, y establecer una la regulación específica de cada uno de estos derechos, en un reglamento que se deberá dictar para tales efectos.

Los derechos arco[188] son el conjunto de derechos personalísimos e independientes a través de los cuales la LOPD garantiza a las personas el

[188] CUIDA TUS DATOS. ¿Qué son los derechos arco? [en línea] <http://www.cuidatusdatos.com/infoderechoarco.html> [consulta 29 de noviembre 2015].

poder de control de sus datos personales, lo que solo es posible y efectivo, imponiendo a terceros una serie de obligaciones.

- Derecho de acceso.

Reconocido en el artículo 15 de la LOPD, artículo 27 y siguientes del RDLOPD y artículo 12 de la Directiva 95/46/CE. El interesado o afectado tiene derecho a obtener gratuitamente información sobre sus datos de carácter personal que aparecen incorporados a un fichero de datos para su tratamiento, así como del origen de esos datos y las comunicaciones de los mismos que se hayan realizado o se prevea realizar en el futuro. Tal información puede suministrarse al interesado mediante su visualización en la pantalla del ordenador o por escrito de cualquier tipo que sea perfectamente legible o inteligible y que no utilice claves o códigos que requieran el uso de dispositivos mecánicos para su lectura o comprensión.

A diferencia de Chile, donde el derecho al acceso no tiene un plazo estipulado para su ejercicio, en España este derecho puede ejercitarse cada doce meses, a menos que el interesado acredite un interés legítimo, en cuyo caso podrá ejercitarlo antes de trascurrir dicho plazo.

- Derecho de rectificación y cancelación.

Frente a un tratamiento de datos, inexacto, incompleto, inadecuado o excesivo, el titular de aquellos datos personales dispone de dos opciones, o bien ejercer su derecho de rectificación o hacer uso del derecho a la cancelación, en cuyo caso los datos quedan bloqueados. Estos derechos están reconocidos en el artículo 16 de la LOPD, artículo 32.2 de la RDLOPD y artículo 112.b de la Directiva 95/46/CE.

- Derecho de oposición.

Reconocido en el artículo 6.4, 17 y 30 de la LOPD, artículos 34 y siguientes de la RDLOPD y artículo 14 de la Directiva 95/46/CE.

Este derecho otorga al interesado la facultad de oponerse por motivo legítimo y fundado al tratamiento de sus datos cuando exista una situación personal concreta, cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial o cuando tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

iv) Control coercitivo y sancionador.

En virtud de lo establecido en el artículo 18 de la LOPD, la tutela de todos estos derechos es asegurada por la Agencia Española de Protección de Datos[189], por tanto, en casos en que el responsable del fichero no respete alguno de los derechos que ya fueron revisados con anterioridad, la persona afectada tiene la facultad de interponer una reclamación ante esta entidad y, si el conflicto no es solucionado por la vía administrativa, el afectado tiene la opción de recurrir a la jurisdicción que corresponda según la titularidad pública o privada del responsable del fichero de datos.

Además es importante señalar que la Agencia Española de Protección de Datos no es competente para referirse al derecho de indemnización en caso que procediere de acuerdo a lo estipulado en el artículo 19 de la LOPD, por tanto el afectado deberá recurrir a la jurisdicción. En caso de que el responsable del fichero sea del área pública se debe recurrir al procedimiento administrativo común[190]; en caso de que el respónsale del fichero sea del sector privado, será componente para conocer de la acción de reclamación de indemnización, la justicia ordinaria[191]. Sin embargo, no

[189] Se profundizará sobre el procedimiento sancionador en el siguiente capítulo.
[190] El cual está establecido en la Ley 30/1992 de 26 de noviembre, de Régimen Jurídico de las administradoras públicas y del procedimiento administrativo común.
[191] CUIDA TUS DATOS. Derecho de indemnización. [en línea]

se profundizará respecto a estos procedimientos por ser temas que exceden al ámbito del presente trabajo.

Para finalizar, respecto al régimen de catálogo de infracción y sanciones frente al incumplimiento de los principios y derechos ya señalados, la LOPD en su título VII regula este tema, entregando a la Agencia Española de Protección de Datos la potestad sancionadora, en virtud de lo establecido en el artículo 37 del mismo cuerpo legal.

En el artículo 44 de la LOPD se señala la existencia de tres tipos de infracciones, las cuales se calificaran en leves, graves o muy graves. Por nombrar algunas, se considerarán como infracciones leves el incumplimiento al principio de información; como infracción grave el incumplimiento al principio de consentimiento y principio de calidad de los datos; y se considerara como infracción muy grave la transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos, salvo excepciones establecidas en la LOPD.

<http://www.cuidatusdatos.com/derechoslopd/indemnizacion/index.html>[consulta: 29 de noviembre de 2015]

Se debe mencionar que, si comparamos las categorías de infracción establecidas en España y Chile, el sistema español impone un sistema más estricto y severo; ejemplo de lo anterior es que en Chile el tratamiento de datos sin consentimiento de su titular configura una infracción grave, mientras que en España está calificada de muy grave. Además, otras diferencias recaen en la diferencia pecuniaria asociada a las multas; pues mientras en Chile las cuantías son consideradas bajas y por tanto irrisorias[192], en España son mayores, teniendo las infracciones leves multas asociadas entre los 900 a 40.000 euros, las graves de 40.001 a 300.000 euros y las muy graves multas de 330.001 a 600.000 euros.

De esta forma, se desprende que al establecer multas de mayor valor pecuniario inhibe al mercado y al Estado, disciplinándolos y por tanto, evitando el incumplimiento de la normativa, pues tanto los particulares como entidades públicos serán más minuciosos en su actuar, con la finalidad de evitar pagar los valores asociados a las multas. Por tanto, nuestro país debiese establecer sanciones más duras y de un valor

[192] Máximo 1.000 UTM, monto que puede disminuir pues el sistema establece atenuantes y mecanismos alternativos a la multa.

pecuniario mayor, por lo que en opinión de esta investigación la reforma chilena en tramitación debiese tener en consideración este tema.

4.3. Ley Orgánica 34/2002.

La Ley 34/2002, del 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, tuvo por objeto incorporar al ordenamiento jurídico Español la Directiva 2000/31/CE sobre el comercio electrónico; por motivos de que la normativa interna imperante no podía regular ciertos actividades realizadas por los medios electrónicos, por su novedad o las peculiaridades que implican su ejercicio por vía electrónica.

Es importante señalar que la Ley 34/2002 es trascendental en el análisis posterior que se realizará en el caso de las redes sociales, pues esta ley se aplica con carácter general en estas plataformas, mientras que la Ley Orgánica 15/1999 y 1/1982 se aplica de forma particular.

La normativa contenida en la Ley 34/2002 se aplica con carácter general en las redes sociales, por motivo de ser consideradas servicios de la sociedad de la información, desde un punto de vista normativo.

En efecto, la Ley 34/2002 señala en su artículo 1° que es la encargada de regular las obligaciones de los prestadores de servicios de la sociedad de la información y de la contratación por vía electrónica.

Se entenderá por servicio de la sociedad de la información aquellos que prestan "servicios a distancia, por vía electrónica y a petición individual del destinatario normalmente a título oneroso"[193]. En síntesis, dentro de la normativa española quedan comprendidos aquellos servicios prestados por internet, siempre que represente una actividad económica para el prestador. Además, la Ley 34/2002 somete a su normativa, de acuerdo a lo señalado en el artículo 2, tanto a los proveedores de servicios de la información establecidos en España y a los servicios prestados por ellos, así como a los prestadores residentes o domiciliados en otros estados, pero que ofrezcan servicios a través de un establecimiento permanente situado en España. Se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en el mismo, de forma continuada o habitual, de instalaciones o lugares de trabajo, en los que realice toda o parte de su actividad. Lo cual tiene trascendencia en el tema de regular las redes sociales, pues es sabido que la mayoría se ubica en

[193] España. Ley 13.758/2002. Anexo Letra A.

diversas partes del mundo, y muchas de ellas, no se encuentran en el territorio de los Estados europeos, por tanto la presente normativa se aplicara de forma parcial a aquellos proveedores que se encuentran fuera de los Estados europeos.

La dictación de esta ley comprueba el nivel de concienciación respecto a la protección de la privacidad y datos personales en España, por motivos de considerar en su regulación esta nueva realidad social surgida con la evolución del internet, imponiendo las bases normativas para una regulación de la red y sus servicios.

Para concluir este capítulo, se debe destacar la importancia de los tratados y convenios para el fortalecimiento de la normativa de protección de datos en España, pues como bien se pudo analizar, impactan tanto en la normativa interna como en la interpretación de la judicatura española. Lo anterior se ve reflejado en que, si bien España destaca dentro de los países europeos por otorgar protección explícita a nivel constitucional al derecho a la privacidad y protección de datos personales, es la labor interpretativa del Tribunal Constitucional la que destaca, por motivo de desarrollar tanto el

concepto de intimidad y protección de datos de carácter personal, adaptándolos al tiempo y cultura actual de España.

Ahora, tanto la normativa contenida en la Ley 5/1982 y como en la 15/1999 demuestran el cumplimiento de España respecto al mandato contenido en su Constitución relativo a otorgar una regulación sectorial a ambos derechos; es más, frente al progreso de las tecnologías han dictado la Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y la Ley 56/2007 de 28 de diciembre de medidas de impulso de la sociedad de la información, la cual ha influenciado en gran manera respecto a tratar de amoldar la normativa existente en el caso de las redes sociales, como se verá en el capítulo que corresponda. Muy por el contrario, nuestro país no cuenta con una ley general que regule el derecho a la vida privada en sede civil, no existe la consagración explícita del derecho a la protección de datos personales a nivel constitucional y nuestra actual normativa en materia de protección de datos es precaria y obsoleta, y por sobre todo ineficiente al no contar con un sistema sancionador satisfactorio. Pero especialmente considerando el hecho de no contar con una Agencia de Protección de Datos que asegure la protección y cumplimiento de los derechos y principios respecto a esta materia.

Esperemos que la normativa española sirva de ejemplo y modelo rector en las próximas decisiones que deberá adoptar nuestro país en materia de privacidad y protección de datos en esta era digital.

IV. LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

1. Generalidades.

No basta con la consagración de un sistema normativo que proteja la intimidad y los datos de carácter personal sin otorgar eficiencia y eficacia a sus disposiciones legales. El sistema será eficiente en la medida que reconozca la existencia de una serie de mecanismos de control, ya sea de índole legal, administrativa o de otra naturaleza, tendientes a resguardar los derechos reconocidos en esta ley. Y será eficaz en la medida que este sistema normativo permita cumplir con sus objetivos, que no son otros que garantizar y proteger las libertades públicas y los derechos fundamentales relacionados con esta materia.

De esta forma, se ha señalado por la comunidad internacional que, para lograr los objetivos anteriormente descritos, es trascendental que el ordenamiento jurídico interno reconozca la existencia de diversos mecanismos de control, los cuales tienen por afán comprobar, inspeccionar y fiscalizar el desempeño de las entidades públicas y sujetos particulares en el cumplimiento de la legislación imperante. Sin embargo, para no salir de

los márgenes del tema, solo se mencionará a grandes rasgos del control jurisdiccional y, en específico, del control realizado por una autoridad autónoma e independiente que, en la generalidad de las legislaciones, lleva el nombre de Agencia de Protección de Datos.

El control jurisdiccional es el mecanismo máximo de control en toda legislación; no obstante, en Europa, la mayoría de las legislaciones de protección de datos personales consagran el control jurisdiccional como un mecanismo de *ultima ratio*, para aquellos casos de mayor problemática o en los cuales se persigue algún tipo de responsabilidad civil. Lo anterior debido a que cuentan con mecanismos de control adicionales a la judicatura, destacando la existencia de una autoridad de control independiente y autónoma, que tiene por objeto promover, controlar y fiscalizar el cumplimiento de los principios y derechos reconocidos en materia de privacidad y datos personales.

Lo anterior es muy distinto a nuestra realidad nacional. En la legislación chilena vigente, desde un punto de vista fiscalizador y sancionador, se otorga como único mecanismo de control el desplegado por nuestra judicatura, pues, al igual que en la mayoría de los países de Latinoamérica,

no contamos con el reconocimiento de una Agencia de Protección de Datos y, por tanto, carecemos de una entidad encargada de hacer cumplir la normativa contenida en la Ley 19.628.

Como se analizó en la experiencia chilena, la actual reforma en tramitación pretende otorgar ciertas facultades a dos entes públicos: el SERNAC y el Consejo para la Transparencia. Estimo que no es lo más razonable, pues contar con una única Agencia Nacional de Protección de Datos otorgaría una serie de beneficios. Estos beneficios se evidencian al describir y analizar la realidad de la Agencia Española de Protección de Datos en el presente capítulo, pues solo de esta forma podremos entender con posterioridad su trascendental importancia en la protección y cumplimiento de su normativa en esta era, en la que predomina el uso de las redes sociales.

2. Origen y fundamento.

En Europa, durante la década de los setenta se instauran las primeras autoridades de control, sin embargo es durante el transcurso de los años 80 cuando este tipo de entidades se masifica, por la entrada en vigencia del Convenio 108.

El Convenio 108 propone a sus Estados miembros contar con una autoridad controladora de fichero. A esta autoridad debiese reconocérsele, por la normativa interna de cada Estado, una serie de facultades destinadas a asegurar y fiscalizar el correcto tratamiento de los ficheros de datos personales. Como consecuencia de lo anterior, España adoptó el criterio organizacional y funcional propuesto por el referido convenio, creando su Agencia de Protección de Datos durante el año 1992, como consecuencia de la entrada en vigencia de la LORTAD.

La LORTAD dedicó todo el capítulo VI a estructurar y describir las principales funciones de esta entidad, destacando como principal finalidad el velar por el cumplimiento de la normativa de protección de datos[194]. Sin embargo, es con la dictación del Real Decreto 428/1993 de 26 de marzo que se aprueba el Estatuto de la Agencia de Protección de Datos (en adelante, EAPD), donde se complementa y especifica la regulación de esta entidad.

Con el transcurso del tiempo y el progreso de las TIC durante la década de los años ochenta y noventa, la comunidad internacional destacó el

[194] AGPD. Historia de la Agencia Española de Protección de Datos. [en línea] <https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/historia-ides-idphp.php>[consulta: 29 de noviembre de 2015]

carácter imperioso de reforzar la protección de datos de carácter personal frente al auge del flujo transfronterizo de datos. De tal forma, la OCDE, si bien en el año 1980, sobresale por la dictación de sus principales "Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales", es debe mencionar que, en el ámbito de las autoridades de control es en el año 2006 donde esta entidad actualiza sus principales directrices y centra sus recomendaciones en fortalecer el rol internacional de las autoridades de control de los diversos Estados miembros. Así, en el documento denominado el *Report on the cross-border enforcement of privacy laws*[195], la OCDE señala los próximos desafíos que deben sortear estas entidades en temas relativos a privacidad. Para tales efectos, destacan las siguientes recomendaciones:

- Las autoridades de control deben replantear la idoneidad de sus sanciones y recursos disponibles a nivel de legislación interna, con el afán de reforzar el resguardo del derecho a la privacidad en el contexto de transferencias de datos internacionales.

[195] OCDE. 2006. Report on the cross-border enforcement of privacy laws. [en línea] <http://www.oecd.org/sti/ieconomy/37558845.pdf> [consulta: 24 de enero de 2016] 46p. (Traducción propia)

- Además, deben investigar nuevos mecanismos de notificaciones, intercambio de información y asistencia investigativa entre ellas, con el fin de mejorar la cooperación a nivel internacional y,

En síntesis, la OCDE insta a todas las autoridades de control a colaborar en la implementación de un estándar adecuado de privacidad homogéneo en todos sus Estados miembros, pues solo de esta forma la transferencia internacional de datos cumplirá con altos estándares de seguridad en esta materia. Para tales efectos, es primordial que cada país adecúe su legislación interna a las recomendaciones realizadas por la OCDE, ya que solo de esta forma, estaremos en presencia de un sistema eficiente y eficaz.

Ahora, por parte de la Unión Europea, esta entidad dicta la Directiva 95/46/CE. En ella realiza una serie de recomendaciones respecto a las principales características que debe tener toda autoridad de control que cumpla con el estándar adecuado de privacidad exigido por la comunidad internacional. En virtud de lo anterior, el artículo 28.3 de la Directiva 95/46/CE señala que estas autoridades de control deben contar con potestades de investigación, intervención y capacidad procesal, en caso de infracciones a las disposiciones de la legislación interna.

Como se analizó en el capítulo anterior, es en virtud de la transposición de la Directiva a la normativa española por la cual se promulgó la LOPD, teniendo como consecuencia la ratificación de la creación de la Agencia Española de Protección de Datos en el artículo 35 de la LOPD, consagrando además una serie de potestades adicionales a las ya reconocidas en la derogada LORTAD. Estas potestades se pueden categorizar en potestades investigativas, fiscalizadoras e incluso sancionadoras, complementándose dicha normativa con el estatuto contenido en el Real Decreto 428/1993, el cual se entenderá vigente en todo aquello que no contradiga a la LOPD.

En síntesis, el régimen jurídico español aplicable a la Agencia Española de Protección de Datos en la actualidad está conformado por la Ley Orgánica 15/1999 (LOPD), el Real Decreto 1720/2007 (RDLOPD), el real Decreto 428/1993 (EAPD) y, en forma supletoria, la Ley 6/1997 de 14 de abril, "Sobre organización y funcionamiento de la administración general del Estado".

Ahora, cabe mencionar que para asegurar que la Agencia Española de Protección de Datos pudiera ejercer sus diversas potestades, de forma

eficiente y eficaz, se le reconoció que en el ejercicio de sus funciones debía realizarlas con plena independencia.

La independencia no se debe interpretar necesariamente en un sentido orgánico, sino que la directiva de la cual España tomó la recomendación hace referencia a la independencia funcional, esto es, que el actuar y decisiones de la Agencia no estén supeditada a ninguna autoridad superior, pues se pretende evitar influencias del gobierno de turno o de otra índole. Esto busca asegurar un correcto y transparente desempeño en su actuar, lo cual se refleja tanto en la estructura orgánica de la Agencia, como en sus principales funciones.

3. Definición.

El artículo 35 de la LOPD define a la Agencia Española de Protección de Datos como 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[196]. Se

[196] AGPD. Funciones Generales. [en línea] <http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/funciones-ides-idphp.php> [consulta: 29 de noviembre de 2015]

complementa esta definición por el artículo 1 del EAPD, señalando que la AEPD se relacionará con el Gobierno a través del Ministerio de Justicia.

De la definición anterior, es posible desprender dos consecuencias. Primeramente, al ser un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada tiene su propio estatuto, contenido en el Real Decreto 428/1993 (en adelante, "EAPD", indistintamente), aplicándosele de forma supletoria la Ley 6/1997 de 14 de abril "Sobre organización y funcionamiento de la administración general del Estado". Sin embargo, en comparación a los demás organismos públicos del Estado, tiene como particularidad ser la única administración edificada en España para la defensa de un derecho fundamental.

En segundo lugar, encontramos el elemento de independencia, el cual se traduce en que ningún ministerio u órgano de la administración tiene facultades que incidan en el actuar de esta entidad. En consecuencia, la relación de la AEPD y Ministerio de Justicia es excepcional y solo de índole informativa, siendo esta la única situación donde un organismo ajeno a la Agencia interviene de alguna forma en representación de esta.

Lo anterior es muy distinto a lo que se pretende impetrar en Chile con la reforma a la Ley 19.628, ya que el SERNAC es un organismo público que está en constante y directa relación con el gobierno, por motivos de ser un servicio público dependiente del Ministerio de Economía, Fomento y Turismo, mientras que el Consejo para la Transparencia si bien goza de cierta autonomía, esta memoria estima que lo más idóneo es contar con una entidad especializada en resguardar la privacidad y datos personales de las personas. Como señala Alberto Cerda solo de esta forma se evita "una pluralidad de entes, ya que fragmenta la protección y da pie a una incoherencia sistémica lo cual nos hace optar por la institución de un único organismo especializado, creado *ex novo* con facultades para velar por el cumplimiento de las disposiciones aplicables al tratamiento de datos personales, sea que él se verifique en (sic) por medios automatizados o no, tanto en el sector público como privado[197]."

[197] CERDA, Alberto. 2003. La autoridad de control. Óp Cit. 238p.

4. Estructura orgánica.

La estructura orgánica de la Agencia Española de Protección de Datos se encuentra consagrada en el artículo 11 del EAPD al señalar que la AEPD se estructura en los siguientes órganos:

- El director de la Agencia de Protección de Datos
- El Consejo Consultivo
- El Registro General de Protección de Datos
- La Inspección de Datos
- La Secretaría General

Finaliza el referido artículo señalando que estos tres últimos órganos son jerárquicamente dependientes del director de la Agencia.

De esta forma, cada organismo integrante de la AEPD tiene una serie de funciones específicas reconocidas por la ley, las cuales permiten asegurar el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

i) Director.

El artículo 36 de la LOPD señala que el director es quien dirige y ostenta la representación de la Agencia. Quien desempeña su cargo con dedicación absoluta, plena independencia y total objetividad.[198] Estando los demás órganos integrantes de la AEPD subordinados jerárquicamente a los preceptos emanados por el director[199].

En virtud de lo anterior, el director es la autoridad máxima de la Agencia Española de Protección de Datos y, en consecuencia, el EAPD en su artículo 16 reitera el elemento de independencia, terminando por especificar que no estará sujeto a mandato imperativo, ni recibirá instrucciones de autoridad alguna. A mayor abundamiento, el elemento de independencia también se refleja en el mecanismo de nombramiento del director[200], así como en las reglas estrictas y excepcionales para removerlo de su cargo[201], con el afán de evitar cualquier intromisión política en su actuar.

[198] PIÑAR, José Luis. 2003. La Agencia Española de protección de Datos: estructura y funcionamiento. Revista Chilena de Derecho Informático (3):31-45.
[199] ESPAÑA. EAPD. artículo 11.2.
[200] Ibíd. artículo 14.
[201] Ibíd. artículo 15.

Ahora, respecto a las principales funciones del director, el EAPD distingue entre funciones de dirección y funciones de gestión, sin embargo solo se hará mención a algunas, pues dicha materia excede el ámbito de esta memoria.

La función de dirección esencial que realiza el director es el dirigir la Agencia y ostentar su representación, además de dictar las resoluciones e instrucciones que requiera el ejercicio de las funciones de la Agencia. De lo anterior, en concordancia con el artículo 16.2 del EAPD, se desprende en simples palabras que el director es la Agencia misma, pues, en su actuar independiente no está subordinado a las decisiones de ningún tipo de autoridad externa ni interna de la propia Agencia.

Dentro de las otras funciones de dirección, se destacan aquellas relacionadas con las potestades de fiscalización y régimen sancionatorio, entre las que se encuentran:

- Resolver motivadamente sobre la procedencia o improcedencia de las inscripciones que deban practicarse en el Registro General de Protección de Datos.

- Adoptar las medidas cautelares y provisionales que requiera el ejercicio de la potestad sancionadora de la Agencia con relación a los responsables de los ficheros privados.
- Iniciar, impulsar la instrucción y resolver los expedientes sancionadores referentes a los responsables de los ficheros privados.

Ahora, respecto a las funciones de gestión, las cuales tienen relación con la ejecución económica-financiera de la Agencia, destacan[202]:

- Ordenar la convocatoria de las reuniones del Consejo Consultivo.

- Aprobar la memoria anual de la Agencia.

Esta última es de trascendental importancia. Tiene por finalidad informar a los ciudadanos de las principales tendencias legislativas, jurisprudenciales y doctrinales en materia de protección de datos, así como realizar un análisis y valoración de los problemas de protección a escala nacional[203]. Lo anterior con el afán de decidir las próximas directrices que deberán implementar en su actuar, destacando en el último tiempo la problemática

[202] PIÑAR, José. Luis. La Agencia Española de protección de Datos: estructura y funcionamiento. Óp. Cit. 36p.
[203] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Memoria 2014. [en línea] <http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2014/Memoria_AEPD_2014.pdf> [consulta 29 de noviembre de 2015]

de internet y las redes sociales, en específico la difusión de imágenes de terceros sin su consentimiento[204].

ii) Consejo Consultivo.

El artículo 18 del EAPD señala que el Consejo Consultivo es un órgano de asesoramiento del director de la Agencia de Protección de Datos. El Consejo Consultivo emitirá un informe en todas las cuestiones que le someta el director de la Agencia de Protección de Datos y podrá formular propuestas en temas relacionados con las materias de competencia de esta.

Es importante señalar que respecto a la relación director y Consejo, es posible comprobar la total independencia del director en su actuar; pues, como señala la normativa, el Consejo es de carácter consultivo y, como tal, queda a discrecionalidad del director si acoge las recomendaciones del Consejo o no.

Es importante aludir al tema de cómo se estructura y elige este consejo, pues lo que busca la legislación española es contar con un órgano democrático y docto en todas las áreas relacionadas a la privacidad y protección de datos personales en general.

[204] Ibíd. 12p.

De acuerdo a lo establecido en el artículo 38 de la LOPD[205], los miembros que componen el Consejo Consultivo son de los más variados sectores, lo cual permite tener una representación transversal y ecléctica, además de configurarse como un organismo especializado en materia de protección de datos, desde una perspectiva política, legislativa, social, cultural y tecnológica. Lo anterior es necesario, puesto que, para asegurar el respeto de la normativa, es importante considerar tres elementos: la innovación, el desarrollo y la investigación[206]. Elementos que son esenciales en esta época tecnológica, pues permiten amoldar la realidad actual a la normativa existente, colaborando a evitar la obsolescencia de las leyes de protección de datos de carácter personal.

iii) Registro General de Protección de Datos.

El Registro General de Protección de Datos se encuentra definido en el artículo 23 del EAPD como aquel órgano de la Agencia de Protección de Datos al que le corresponde velar por la publicidad de los ficheros

[205] El consejo estará compuesto por un diputado, un senador, un representante de la administración central y local, un miembro de la Real Academia de la Historia, un experto en la materia, un representante de los usuarios y consumidores, un representante de cada comunidad autónoma que haya creado una agencia de protección de datos y un representante del sector de ficheros privados.

[206] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. Óp. Cit. 10p.

automatizados de datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos. Es importante señalar que este órgano es una novedad de la normativa española, pues la Directiva 95/46/CE no imponía la creación de un órgano con tales características.

Dentro de las funciones que se pueden resaltar del registro, destacan las siguientes[207]:

- Instruir las inscripciones y certificaciones los expedientes de inscripción de ficheros automatizados de titularidad pública y privada[208].

En el caso de Chile es el Servicio de Registro Civil e Identificación, que lleva un registro de los bancos de datos personales[209], pero solo limitándose a los de titularidad pública, careciendo nuestro país de un registro de bancos de datos personales de titularidad privada. Lo señalado, tiene como consecuencia para los ciudadanos la mayor complejidad de ejercer sus

[207] PIÑAR, José Luis. La Agencia Española de protección de Datos: estructura y funcionamiento. Óp. Cit. 38p.
[208] ESPAÑA. EAPD. artículo 26.
[209] Chile. Ley 19.628. artículo 22.

derechos arco ante estas entidades, pues al no existir un registro de ficheros privados difícilmente sabrán quiénes y qué datos tienen estas instituciones.

- La autorización de transferencias internacionales[210].

La normativa española establece que solo se podrán realizar transferencias internacionales de datos respecto a aquellos países[211] que consideren que cumplen con un adecuado estándar de privacidad; permitiéndose solo de forma excepcional y después de un exhaustivo estudio, con autorización del director de la Agencia, la transferencia internacional de datos a países que no cumplen con este estándar de privacidad. Así ocurre en el caso de Chile, al no contar con una Agencia de Protección de Datos y frente a la serie de falencias que posee nuestra actual normativa, la comunidad europea estima que nuestro país no cumple con el estándar adecuado de privacidad.

---

[210] Las transferencias internacionales de datos, son tratamientos de datos que implican una transmisión de los mismos a un países no perteneciente al Espacio Económico Europeo, tanto por la vía de la cesión de datos como cuanto tenga por objeto la realización de un tratamiento de datos por cuenta del Responsable del Fichero establecido en territorio español.

[211] AGPD. Protección de datos en el mundo.
[en línea]
<http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/index-ides-idphp.php>[consulta: 29 de noviembre de 2015].

En conclusión, la labor del Registro General de Protección de Datos es trascendental, ya que los principios de información y finalidad se ven claramente reflejados en esta institución. En efecto, en la medida en que se permite a los ciudadanos estar en conocimiento de la existencia de ficheros tanto de titularidad pública como privada, posibilita que estos puedan ejercer sus derechos arco en aquellos casos en que lo estimen convenientes. Lo anterior es un claro ejemplo de como se le otorga eficacia y eficiencia a la normativa.

iv) Secretaría General.

De acuerdo a lo establecido en los artículos 30 y 31 del EAPD, cumple una serie de funciones de apoyo y ejecución, las cuales son delegadas por el director cuando la ley lo faculta para esto[212]. Destaca entre ellas: la elaboración de informes y propuestas que le solicite el director, notificar las resoluciones del director, ejercer la secretaría del Consejo Consultivo y editar los repertorios oficiales de ficheros inscritos, las memorias anuales y cualquier otra publicación de la AEPD. Asimismo, la Secretaría General es

[212] España. EAPD. artículo 13.2.

la encargada de facilitar la información necesaria para llevar a cabo campañas de difusión a través de los medios de comunicación.

v) Inspección de Datos.

De acuerdo al artículo 27 del EAPD, la Inspección de Datos es el órgano de la Agencia de Protección de Datos al cual le competen las funciones inherentes en el ejercicio de la potestad de inspección que el artículo 40 de la LOPD atribuye a la Agencia.

De esta forma, a esta entidad le corresponde ejercer la función de inspección[213], la cual consiste en examinar y requerir el acceso a los ficheros de datos personales, tanto de titulares públicos como privados, con la finalidad de asegurar el correcto cumplimiento de la ley por parte de los responsables de los ficheros de datos. En caso de incumplimiento de la normativa, puede requerir toda información precisa para el ejercicio de su función instructora, que se traduce en obtener información y pruebas sobre posibles incumplimientos a la LOPD.

[213] Ibíd. artículo 27.

Asimismo, esta función instructora, como señala el exdirector de la AEPD don José Luis Piñar Mañas[214], se traduce en la incoación de tres clases de procedimientos: el procedimiento por infracciones de las administraciones públicas, el procedimiento sancionador contra los responsables de ficheros de titularidad privada por infracción a los principios de los principios y reglas contenidos en la LOPD y el procedimiento de tutela de derechos previsto en el artículo 18 de la LOPD.

Estos procedimientos serán analizados al final del presente capítulo (exceptuando el procedimiento por infracción de las administraciones públicas que excede al tema de esta tesis), enfocándonos en el ámbito privado.

5. Estructura funcional.

En cuanto a la estructura funcional de la AEPD, es preciso señalar que la primera sistematización[215] fue realizada por el Tribunal Constitucional en la Sentencia 290/2000, al categorizar sus potestades en el siguiente tenor:

[214] PIÑAR, Jose Luis. La Agencia Española de protección de Datos: estructura y funcionamiento. Óp. Cit. 41p.

[215] La ley no establece una clasificación objetiva. En efecto, existen diversas clasificaciones construidas por la doctrina y por la AEPD.

- Potestad de investigación o inspección: tiene por finalidad obtener información y, en su caso, pruebas sobre hechos que contravengan lo dispuesto en la LOPD (artículo 40).

- Potestad sancionadora la Agencia de Protección de Datos ha de ejercerla en los términos previstos en el título VII, con la salvedad que cuando se trate de infracciones de la Administración Pública tal potestad queda limitada a la facultad de dictar una resolución indicando las medidas que han de adoptarse para corregir el incumplimiento de las previsiones legales en esta materia.

- Potestad de resolución de las reclamaciones de los afectados por incumplimiento de las previsiones de dicha ley (artículo 37.D de la LOPD).

- Potestad normativa: ceñida en lo esencial a dictar las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la LOPD (artículo 37 letras C y M de la LOPD).

Si bien existen diversas formas de clasificar las funciones de la AEPD, he de analizar a continuación la sistematización que se infiere del propio

EAPD, y, por tanto, señalado por la propia Agencia en su actuar[216]. Realizándose esta clasificación en consideración de los actos y actores involucrados:

i) En relación con los afectados.

- Atender a sus peticiones y reclamaciones.

- Informar de los derechos reconocidos en la ley.

- Promover campañas de difusión a través de los medios.

- Velar por la publicidad de los ficheros de datos de carácter personal.

La atención a las peticiones y reclamaciones de los afectados se manifiesta en dos procedimientos encargados a la AEPD, es decir, el Procedimiento de Tutela de Derechos y el Procedimiento de Denuncias por infracción a la normativa contenida en la LOPD.

Con la finalidad de facilitar el ejercicio de sus derechos a los afectados la AEPD ha implementado formularios electrónicos, a través de los cuales pueden solicitarse los procedimientos anteriormente citados. Para tales

[216] AGPD. Funciones Generales. [en línea] <http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/funciones-ides-idphp.php> [consulta: 29 de noviembre de 2015]

efectos creó la "Sede Electrónica"[217], una plataforma que ha puesto en marcha la Agencia Española de Protección de Datos a través de la cual se facilita el acceso electrónico de los ciudadanos a los servicios públicos tal y como establece la Ley 11/2007 , de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Asimismo, para informar a los ciudadanos de sus derechos reconocidos en la ley, la AEPD ha habilitado el "Canal Ciudadano"[218]. Mecanismo por el cual el ciudadanos puede realizar diversas consultas atingente a este tema, ya sea por vía telefónica, presencial, por escrito o por sede electrónica. Respecto al año 2014 se realizaron un total de 99.524 consultas ciudadanas, siendo satisfactoriamente resueltas el 98% de ellas[219].

A mayor abundamiento, la AEPD ha realizado diversas campañas de difusión en los medios respecto a los derechos que los ciudadanos tienen, así como una serie de recomendaciones para proteger la privacidad en las plataformas tecnológicas, haciendo énfasis en el resguardo de los derechos de los sectores más vulnerables, como son los menores de edad.

[217] SEDEAGPD. ¿Qué es la sede? [en línea] <http://www.sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/queSede.jsf>[consulta: 29 de noviembre 2015].
[218] AGDP. Canal del Ciudadano [en línea] <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/index-ides-idphp.php> [consulta: 29 de noviembre de 2015]
[219] Ibíd.

Asimismo, la relación que ha surgido entre la AEPD y los diversos medios de comunicación ha tenido como consecuencia la sensibilización a la protección de datos personales por estos medios, lo cual claramente se ve reflejado en que gran parte de las investigaciones de oficio que ha llevado a cabo la AEPD tienen su origen en informaciones de medios de comunicación que, por su trascendencia social han exigido la actuación de la Agencia[220].

Respecto a la publicidad de los ficheros, la AEPD ha facilitado en su sitio web un buscador de ficheros de datos, lo cual permite al ciudadano saber qué y quién está tratando sus datos, lo cual tiene por consecuencia permitir al ciudadano solicitar la protección de sus derechos arco.

ii) En relación con quienes tratan datos.

- Emitir autorizaciones previstas en la ley.
- Requerir medidas de corrección.
- Ordenar, en caso de ilegalidad, el cese del tratamiento y la cancelación de los datos.

[220] RALLO, Artemi. 2009. La protección de datos en España: análisis de actualidad. Anuario de la Facultad de Derecho (2):5-30.

- Ejercer la potestad sancionadora.

- Recabar de los responsables de los ficheros la ayuda e información que precise para el ejercicio de sus funciones.

- Autorizar la transferencia internacional de datos.

- Colaborar con los responsables de datos o encargados para lograr el cumplimiento de la ley.

De las funciones anteriormente mencionadas, la relación entre la AEPD y quienes tratan datos es, básicamente, de índole fiscalizadora y coercitiva. Sin embargo, como señala Agustín Puente Escobar[221], se debe destacar la importancia de la última de las funciones mencionadas, esto es, la colaboración con los responsables de datos o encargados para lograr el cumplimiento de la ley, lo que se traduce en el ejercicio por parte de la AEPD de la potestad preventiva.

Además, la potestad preventiva se traduce en garantizar el derecho a la protección de sus datos mediante la educación y difusión a los ciudadanos de los principales peligros que conlleva el sobreexponer la privacidad de los

[221] PUENTE, Agustín. 2008.La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal. Azpilcueta: Cuadernos de Derecho (20):13-41.

datos en la época actual, pues lo ideal es que las reclamaciones que lleguen a la AEPD sean de trascendental gravedad, tales como estafas informáticas, suplantación de identidad, etc. Es decir, situaciones que son difíciles de controlar sobre todo en el ámbito de internet, y en específico en las redes sociales.

iii) En la elaboración de normas.

- Informar preceptivamente los proyectos de normas de desarrollo de la Ley Orgánica de Protección de Datos.
- Informar los proyectos de normas que incidan en materia de protección de datos.
- Dictar las instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica de Protección de Datos.
- Dictar recomendaciones de aplicación de las disposiciones legales y reglamentarias en materia de seguridad de los datos y control de acceso a los ficheros.

La función normativa de la AEPD ha permitido su directa colaboración con diversos sectores relacionados a esta materia, resguardando de forma

activa el derecho a la protección de datos personales. Así, desde el punto de vista legislativo, el papel de la Agencia Española de Protección de Datos ha sido trascendental, pues ha colaborado en la dictación de diversas normativas relacionadas con la protección del derecho a la protección de datos personales, desde diversas áreas, tales como el comercio electrónico, telecomunicaciones, sanidad, entre otras[222].

Como señala el exdirector de la AEPD, Artemi Rallo Lobarte: "Facilitar el cumplimiento de la LOPD es un objetivo que se complementa con la actividad dirigida a conseguir una mejor sistemática en las regulaciones sectoriales que puedan incidir en la protección de datos personales"[223].

Asimismo, desde el punto de vista jurisprudencial, con la intención de reforzar la protección de este derecho, la AEPD ha suscrito un convenio[224] con el Poder Judicial, el cual tiene por finalidad mejorar el servicio que cada institución ofrece en el ejercicio de sus respectivas competencia, así

[222] Ibíd. 31p.
[223] RALLO, Artemi. La protección de datos en España: análisis de actualidad. Óp. Cit. 20p.
[224] CONSEJO GENERAL DEL PODER JUDICIAL Y AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Convenio de 13 de julio de 2015 [en línea] <https://www.agpd.es/portalwebAGPD/LaAgencia/gestion_economica/convenios/common/Convenio_CENDOJ-AEPD.pdf> [consulta: 29 de noviembre de 2015]

como realizar diversos estudios en conjunto en materia de protección de datos y tratamiento de información jurídica.

Y, para finalizar, desde el ámbito internacional, la AEPD es parte integrante del Grupo de trabajo 29 de la Directiva 95/46/CE, por tanto, ha participado activamente en la investigación y diversas propuestas para regular áreas específicas de esta materia, destacando su participación en la elaboración del Dictamen 5/2009 sobre redes sociales, el cual procederemos a analizar en el próximo capítulo.

iv) En materia de telecomunicaciones.

- Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente (spam).

- Recibir las notificaciones de los eventuales quiebres de seguridad que se produzcan en los sistemas de los proveedores de servicios de comunicaciones electrónicas y que puedan afectar a datos personales.

En consecuencia, como las redes sociales son un servicio de la sociedad de la información desde la perspectiva legal, esta función refuerza la trascendental labor de la AEPD en el ámbito de estas plataformas virtuales, al potenciar desde el ámbito legal, contenido en la Ley 34/2002, el *ius puniendi* que puede ejercer contra este tipo de servicios en caso de que no ofrezcan una adecuada seguridad a los datos de sus usuarios o envíen spam a sus usuarios, entre otras situaciones contempladas por la normativa.

Para finalizar, destacan otras funciones que no se sistematizan en alguna de las clasificaciones anteriores, pero que son trascendentales, tales como la cooperación con diversos organismos internacionales y con los órganos de la Unión Europea en materia de protección de datos, la representación de España en los foros internacionales en la materia y la elaboración de una memoria anual, que es presentada por el director de la Agencia ante las Cortes.

6. Principales procedimientos tramitados por la Agencia Española de Protección de Datos.

El procedimiento de tutela de derechos y el procedimiento sancionador son los dos principales procedimientos que, en virtud de lo consagrado en el

artículo 18 y artículo 48 LOPD, deben ser tramitados por la Agencia Española de Protección de Datos.

Durante el transcurso del año 2014 la AEPD recibió 2.099 solicitudes de procedimiento de tutela de derechos[225] y 10.074 solicitudes por infracción[226] a la LOPD, siendo resueltas el 87% de las solicitudes de tutela de derechos y 93% de los reclamos realizados por infracción a la LOPD, cifras que arrojan un índice positivo respecto al funcionamiento de la AEPD como ente fiscalizador y sancionador.

En efecto, si bien la cantidad de reclamos ha aumentado por motivo del auge de las TIC y las múltiples posibilidades de tratamiento indebido de datos que estas conllevan, este aumento también debe analizarse desde una perspectiva positiva. En este sentido, los diversos mecanismos implementados por la AEPD han tenido como consecuencia que los ciudadanos españoles han adquirido conciencia de lo trascendental que es el resguardo de la privacidad de sus datos y de la importancia de conocer los

[225] Agencia Española de Protección de Datos. Ejercicio de Derechos. [en línea] <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/ejercicio_derechos/index-ides-idphp.php> [consulta: 29 de noviembre de 2015]
[226] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Denuncias presentadas. [en línea] <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/denunciasciudadano/index-ides-idphp.php> [consulta: 29 de noviembre de 2015]

derechos les asisten en esta materia. Asimismo, la Sede Electrónica ha sido trascendental para agilizar la interposición de las denuncias y reclamos de los ciudadanos ante la AEPD, quienes no tienen que considerar los costos económicos y procesales para la interposición de una reclamación, como ocurre en Chile.

A continuación se procederá a describir estos dos procedimientos principales tramitados por la AEPD, lo cual nos permitirá entender el funcionamiento administrativo-procesal de la Agencia, y así poder comprender las ventajas de contar una etapa prejudicial, de índole administrativa, para la resolución de estos conflictos.

6.1. Procedimiento de tutela de derechos.

Este procedimiento se encuentra reconocido en el artículo 18 de la LOPD y regulado en el capítulo II del RDLOPD. Consiste en el derecho que tiene el afectado de reclamar ante la Agencia Española de Protección de Datos Personales cuando a criterio del afectado los responsables y encargados[227] del tratamiento de los ficheros, tanto públicos como privados,

[227] A diferencia de la directiva, la ley española distingue entre responsable del fichero como aquella entidad que trata datos personales de forma directa para su actividad comercial o profesional y, por otro, el encargado del tratamiento que corresponde a aquella entidad que trata datos personales por encargo del responsable.

hayan realizado actuaciones contrarias a la ley. En específico cuando se le ha denegado por parte del responsable o encargado del fichero[228], de forma total o parcial, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación o se ha incumplido el deber de respuesta por parte del responsable o encargado del fichero, respecto al acceso, denegación o imposibilidad de efectuar su requerimiento.

El procedimiento se iniciará siempre a instancia del afectado, quien deberá expresar con claridad el contenido de su reclamación y de los preceptos de la LOPD que estime vulnerados. Recibida la reclamación por la AEPD, se dará traslado de la misma al responsable del fichero para que en el plazo de quince días, formule las alegaciones pertinentes. Presentadas las alegaciones o transcurrido el plazo previsto anteriormente, la AEPD previo informes, pruebas y otros actos de instrucción pertinentes, incluida la

[228] La legislación establece que para ejercer estos derechos es imprescindible que el ciudadano se dirija en primer lugar a la entidad que está tratando sus datos utilizando cualquier medio que permita acreditar el envío y la recepción de la solicitud. Si la entidad no responde a la petición realizada en el plazo establecido por ley o el ciudadano considera que la respuesta que recibe no es la adecuada, puede solicitar que la Agencia Española de Protección de Datos tutele su derecho frente al responsable.
AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Ejercicio de Derechos. [en línea]
<http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/ejercicio_derechos/index-ides-idphp.php> [consulta: 29 de noviembre de 2015]

audiencia con el afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada.

El plazo máximo para dictar y notificar la resolución en el procedimiento de tutela de derechos será de seis meses, a contar de la fecha de entrada en la AEPD la reclamación del afectado.

En caso de que la AEPD estime la reclamación del afectado, instará al responsable o encargado de datos, si aún no ha cumplido con lo solicitado por el titular, que en el plazo de 10 días hábiles siguientes a la notificación de la resolución del procedimiento de tutela de derechos remita al reclamante certificación en que haga constar que ha atendido a su derecho de acceso, rectificación, oposición o cancelación según sea el caso, o remita al reclamante certificación en la que se haga constar las causas por las que no procede considerar su derecho, pudiendo incurrir en su defecto en una de las infracciones prevista en el artículo 44 de la LOPD. Asimismo las actuaciones que realice el responsable o encargado del fichero también deberá comunicárselas en el mismo plazo a la AEPD.

Contra la resolución del Director de la Agencia Española de Protección de Datos es posible interponer recurso contencioso administrativo.

6.2. Procedimiento sancionador.

El procedimiento sancionador se encuentra consagrado en el artículo 48 de la LOPD señalando que, por la vía reglamentaria, se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que se hace referencia en el presente aparado, lo cual se concreta en el capítulo III del RDLOPD.

Este procedimiento puede iniciarse de tres formas, ya sea por previa denuncia; por petición razonada de una administración pública o de oficio; o, por iniciativa propia de la AEPD ante sospechas de infracción a la normativa contenida en la LOPD , en específico, en su título VII[229].

i) Actuaciones previas.

Antes de iniciar el procedimiento sancionador, el RDLOPD establece que se deben realizar ciertas actuaciones de forma previa, las cuales tendrán una duración máxima de 12 meses desde que la AEPD acordase su realización o desde la denuncia o petición.

[229] MARTÍNEZ, Eulalia. 2014. El procedimiento sancionador en la Agencia Española de Protección de Datos. Editorial Economist & Jurist. 22(180):20-27.

La finalidad de estas actuaciones previas es determinar si concurren las circunstancias que justifiquen un procedimiento sancionador, así como concretar si se opta por iniciar el procedimiento.[230]

Estas actuaciones se llevarán a cabo de oficio por la AEPD, ya sea por iniciativa propia o como consecuencia de la existencia de una denuncia o petición razonada por otro órgano. Cuando las actuaciones se lleven a cabo como consecuencia de la existencia de una denuncia o de una petición razonada de otro órgano, la Agencia Española de Protección de Datos acusará recibo de la denuncia o petición, pudiendo solicitar cuanta documentación se estime oportuna para poder comprobar los hechos susceptibles de motivar la incoación del procedimiento sancionador. Esto porque el elemento de prueba es un requisito esencial para dar apertura al procedimiento sancionador.

Es en esta instancia previa donde la labor de la Inspección General de Datos es trascendental, pues es el órgano encargado de inspeccionar y recabar cualquier tipo de información, con la finalidad de que el director de la Agencia decida la procedencia de iniciar el procedimiento sancionador.

[230] Ibíd. 22p.

En caso de que el director estime que no existe indicio suficiente que motive la infracción, dictará resolución de archivo de las actuaciones, notificando a todos los interesados e investigados.

ii) Inicio del procedimiento sancionador.

En caso que el director decida que existen indicios suficientes para sospechar de alguna infracción a la LOPD, dictará el acuerdo de inicio del procedimiento sancionador[231].

Sin embargo, en casos excepcionales y tras previa audiencia de los interesados, el director puede decidir no iniciar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto a que acredite en un plazo determinado que ha adoptado las medidas correctoras pertinentes, esto siempre que los hechos fuesen constitutivos de una sanción leve o grave y que el infractor no hubiese sido sancionado o apercibido con anterioridad. Si el apercibimiento no se atiende en el plazo requerido, se procederá a la apertura del procedimiento sancionador.

Siguiendo a Eulalia Martínez, este procedimiento como cualquier otro debe inspirarse en los principios de contradicción, por lo que será necesario

[231] ESPAÑA. RLOPD. artículo 127.

notificar al supuesto infractor del acuerdo para que pueda formular las alegaciones que estime pertinente[232] y, además, se procederá a la apertura de un periodo de prueba para que las partes integrantes del procedimiento presenten aquellas que consideren oportunas.

Es importante señalar que esta etapa probatoria no está regulada en la LOPD ni en el RDLOPD, por tanto, se deberán aplicar de forma supletoria las normas administrativas, que establecen un plazo de 15 días para presentar alegaciones y proponer prueba. Tras la recepción de la prueba o transcurrido este tiempo, el director acordará la apertura de prueba en un plazo que no podrá ser superior a 30 días ni inferior a 10, estimando o desestimando las pruebas.

Una vez notificada la propuesta de resolución a las partes, se abrirá un nuevo periodo de alegaciones. Debido a que el RDLOPD no fija ningún plazo para dictar la resolución, debe entenderse que, transcurridos seis meses desde el Acuerdo de inicio sin que se haya dictado resolución expresa, se procederá a la caducidad del procedimiento y archivo de las actuaciones, en virtud de lo establecido en el artículo 128 del RDLOPD.

[232] MARTÍNEZ, Eulalia. El procedimiento sancionador en la Agencia Española de Protección de Datos. Óp. Cit. 24p.

Después de todo lo descrito y analizado en este capítulo, podemos atestiguar las grandes diferencias entre la normativa española y chilena en materia de protección de datos, sobre todo en lo que respecta a las potestades coercitivas y sancionadoras. Como hemos visto, para que un sistema normativo sea eficiente y eficaz debe ir asociado al reconocimiento de un poder coercitivo y de un poder sancionador. En efecto, la coerción tiene por finalidad propender al cumplimiento de la normativa y el mecanismo principal para asegurar su cometido es reconocer una serie de sanciones que impetrar en caso de incumplimiento a la ley, existiendo por tanto una relación de causa-consecuencia entre ambas potestades. Sin embargo, no basta con la consagración de una serie de potestades si no existe una entidad que las pueda materializar en la vida cotidiana, siendo este el principal motivo por el cual en Chile nuestra normativa es en gran medida ineficaz e ineficiente, en comparación a la experiencia de España.

En conclusión, de la experiencia de la Agencia Española de Protección de datos se puede esprender lo siguiente:

- Para que una autoridad de control pueda ejercer de forma eficiente y eficaz las potestades que se le reconocen en la normativa, es

trascendental que se le reconozca independencia funcional, pues solo de esta forma se pueden evitan las influencias y restricciones que terceros pudieran ejercer sobre la Agencia en su actuar.

- Los diversos órganos que estructuran la AEPD reflejan la especialización de esta Entidad en temas relacionados con la protección de datos personales. Cuenta con diversos expertos en la materia, desde una perspectiva legal, cultural, social y tecnológica, lo cual es trascendental pues, como hemos observado en capítulos anteriores, este derecho muta con el transcurso del tiempo, por tanto sus principales alcances y contenidos jurídicos han sido construidos considerando la realidad cultural y social de la época.
- De las potestades investigativa, sancionatoria, resolutiva y normativa se estructuran las principales funciones de la AEPD, con cuyo ejercicio ha influenciado en forma positiva en el comportamiento de los diversos actores involucrados en materia de protección de datos. Destacando la labor preventiva ejercida por la AEPD ante el incumplimiento de la normativa, pues la Agencia ha dejado claro que busca ejercer sus potestades coercitivas y sancionadoras solo en casos de *ultima ratio*, buscando siempre el consenso entre el afectado y el

responsable de los ficheros en caso de transgresión a algún derecho arco o infracción a la LOPD.

Como se adelantó, la labor preventiva adquiere relevancia en las redes sociales, pues el ejercicio del control coercitivo y sancionador en estos espacios se hace más complejo, por tanto, la difusión y educación en materia de protección de datos personales tanto a los usuarios, como a los proveedores de estas plataformas es primordial.

Asimismo, la AEPD en virtud de sus diversas resoluciones, requerimientos, guías educativas y principales recomendaciones en temas de contingencia ha cooperado con diversos sectores legislativos, tanto a nivel internacional como nacional, para la implementación de una normativa actualizada en protección de datos personales y, de esta forma, hacer frente a las nuevas amenazas que han surgido contra la privacidad y datos de carácter personal, las cuales en su mayoría se deben al uso de internet.

Es en virtud a estas consideraciones que esta investigación estima que Chile debiese contar con una autoridad de control, materializada en una Agencia de Protección de Datos. Es necesario señalar que con esto no se

afirma que debiese ser implementado el mismo modelo español, ya que se debe estructurar una agencia que se base en la realidad de nuestro país, respetando para todos los efectos los elementos esenciales que toda autoridad de control debe tener, tal como independencia funcional, potestades de fiscalización, coerción, sanción y por sobre todo prevención. Al mismo tenor, Alberto Cerda ha señalado que dicha entidad, con miras a potenciar su independencia, debiese ser un organismo colectivo integrado por los tres poderes del Estado: legislativo, ejecutivo y judicial; además, de algunos expertos en la materia[233]. Asimismo, ante la conocida realidad geográfica de nuestro país, es necesario contar con agencias regionales en las principales ciudades de Chile. Estas agencias regionales, subordinarán su actuar y rendirán informe a la Agencia Nacional de Protección de Datos. Lo anterior es primordial, pues solo de esta forma se entregará una atención expedita y eficaz a las peticiones efectuadas por los ciudadanos, además de tener un mayor control en la fiscalización e inspección de los responsables de ficheros y bancos de datos a lo largo del país. En concordancia con lo anterior, se debe incentivar la tramitación electrónica en todos aquellos sectores de difícil acceso a las oficinas regionales. Para finalizar, es

[233] CERDA, Alberto. 2003. La autoridad de control. Óp Cit. 240p.

primordial la difusión, asistencia y promoción de las disposiciones legales y reglamentarias aplicables al tratamiento de datos personales entre la ciudadanía. Para tales efectos, la Agencia Nacional de Protección de Datos debe establecer una alianza estratégica con el Poder Judicial con la finalidad de cumplir con la difusión y promoción de los derechos arco y principales obligaciones de los responsables de ficheros y bancos de datos; además dicha colaboración permitirá colaborar con la judicatura en la comprensión de los principales criterios y alcances actuales del derecho a la vida privada en nuestra realidad nacional.

V. LAS REDES SOCIALES.

1. Origen y fundamento.

Desde un punto de vista tecnológico, las redes sociales surgen como consecuencia del fenómeno llamado la Web 2.0, o mejor conocida como "web colaborativa". En ella, el universo web deja de ser un lugar pasivo y se convierte en un espacio social dinámico[234], siendo el usuario final de internet quien desarrolla este universo digital mediante su participación e interacción con los demás usuarios del ciberespacio[235].

El fundamento de las redes sociales se remonta a la teoría de los seis grados de separación[236], la cual señala que cualquier individuo puede estar conectado a cualquier otra persona del planeta, a través de una cadena de

[234] RALLO, A. y MARTÍNEZ, R. 2011. Protección de datos personales y redes sociales: obligaciones para los medios de comunicación. Quaderns del CAC 37, 14 (2):41-52. p.42.

[235] Para mayor información consultar CALDEVILLA DOMÍNGUEZ, David. 2010. Las Redes Sociales. Tipología, uso y consumo de las redes 2.0 en la sociedad digital actual. Documentación de las Ciencias de la Información, (33):45-68. [en línea] <https://revistas.ucm.es/index.php/DCIN/article/viewFile/DCIN1010110045A/18656> [consulta: 29 de noviembre 2015]

[236] Teoría propuesta en el año 1929 por el escritor Frigyes Karinthy, quien dice que es posible acceder a cualquier persona del planeta en tan solo seis saltos. Sin perjuicio que científicos de la Universidad de Milán han comprobado mediante Facebook que la distancia es de 4,74 y para probarlo usaron los datos de los 721 millones de usuarios que existen. En Twitter, la distancia promedio es de 4,67.

conocidos con no más de cinco intermediarios, aumentando la cifra de conocidos en la medida que lo hacen los eslabones de la cadena. Sin embargo, con el auge de las redes sociales se ha llegado a considerar que el grado de separación es menor, debido a la posibilidad que otorgan estas de expandir dicho círculo.

Desde el ámbito normativo, el desarrollo de la Web 2.0, y en específico de las redes sociales, ha traído consigo dos consecuencias. En primer lugar, estamos viviendo un acelerado proceso de transformación en los paradigmas de lo público y lo privado[237]; y, por otro lado, el desarrollo de las redes sociales ha conllevado un aumento de la recolección y tratamiento indebido de los datos personales.

De lo anterior, no se pretende poner en duda los beneficios y contribuciones de las redes sociales en la vida diaria, sin embargo, corresponde señalar que su masificación, ha conllevado al aumento de las amenazas contra la privacidad y a los datos personales en la red.

---

[237] BAYTELMAN, Paloma. Protección de datos personales en la sociedad en redes. [en línea] <http://www.expansiva.cl/media/en_foco/documentos/18052011161648.pdf>[consulta: 29 de noviembre 2015]

2. Definición.

El estudio realizado por la AEPD y la INTECO[238] define a las redes sociales online[239] como aquellos servicios prestados a través de internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al ser publicados. Mientras que el Grupo de Estudio del Artículo 29 del Consejo de Europa define a las redes sociales como "plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes"[240].

De ambas definiciones, se pueden desprender los tres principales elementos que conforman una red social.

En primer lugar, el elemento esencial de las redes sociales es la comunicación. Como señala Víctor Drummond, la trascendencia de la

[238] AEPD www.agpd.cl; Instituto Nacional de Tecnologías de la Comunicación www.inteco.es.

[239] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. Óp. Cit. 6p.

[240] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 5/2009 sobre redes sociales en línea. [en línea] <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf> [consulta: 29 de noviembre 2015]

comunicación radica en que le confiere más peso a su personalidad, ya que el hombre se desarrolla socialmente desde la comunicación, siendo, por tanto, imperioso proteger y buscar cobijo en el mundo del derecho para la comunicación, en un grado igual o superior que para la información[241].

El usuario de las redes sociales, en razón de querer comunicarse, muchas veces se despreocupa, e incluso ignora su privacidad, compartiendo una serie de informaciones de índole personal, con el objeto de poder acceder y participar en esta sociedad digital.

El segundo elemento es la identidad. En efecto, los datos personales que conforman nuestra identidad como individuo son la moneda de cambio para poder ingresar y participar en estos servicios, siendo por tanto errónea la creencia de que el uso de estas plataformas es gratuito. Aun cuando, por regla general, no se transa dinero en ellas, el individuo otorga sus datos personales e incluso sus datos sensibles, lo cual conlleva una serie de amenazas y usos mal intencionados de ellos, pues otorgan la posibilidad de

[241] DRUMMOND, Víctor. Internet, Privacidad y Datos personales. Óp Cit. pp. 42 y ss.

crear perfiles genéricos de navegación con un determinado valor de mercado[242].

Finalmente, resulta importante la interconectividad, ya que este elemento tiene como consecuencia que la comunicación en las redes sociales se desarrolle de forma masiva, instantánea y retroalimentiva. Lo señalado tiene como principal resultado que la relación entre los usuarios de las plataformas de redes sociales se transforma de vertical a horizontal, lo cual permite que los usuarios sean a la vez transmisores y receptores de información. Esto, a nivel jurídico, tiene como consecuencia que, en ciertos casos, el usuario común de las redes sociales puede llegar a ser responsable del tratamiento de datos al mismo nivel que un proveedor de redes sociales o desarrollador de aplicaciones.

3. Clasificaciones.

El usuario de las redes sociales, al momento de decidir registrarse y participar en una determinada plataforma virtual, toma en consideración dos elementos. Por una parte ha de considerar los intereses comunes que tiene con los otros usuarios y por otra, busca satisfacer una determinada

[242] RALLO, A. y MARTÍNEZ, R. Protección de datos personales y redes sociales: obligaciones para los medios de comunicación. Óp. Cit. 42p.

necesidad mediante su uso. Debido a estas consideraciones, las redes sociales también se clasifican en distintos tipos[243]:

- Redes sociales de comunicación o de ocio: destacan Facebook, MySpace, Tuenti y Twitter[244]. La finalidad de este tipo de redes sociales consiste en facilitar y potenciar las relaciones personales entre los usuarios que la componen[245]. De esta forma, estas redes sociales son las que cuentan con mayor cantidad de usuarios en todo el mundo; destacando la utilización de diversas aplicaciones dentro de la red social con la finalidad de compartir con los demás usuarios fotografías, vivencia, aficiones, preferencias, etc. Además, de ofrecer la posibilidad de comunicarse de forma más privada, por intermedio de un sistema de mensajería instantánea.

- Redes sociales de intercambio de contenido e información: destacan YouTube y Twitter. Tienen por objetivo la publicación de diversos

[243] GIL, Ana. 2012. El fenómeno de las redes sociales y los cambios en la vigencia de los Derechos Fundamentales. España. Revista de derecho UNED 10: 209-255.
[244] Según la finalidad del usuario, puede ser buscar comunicarse por intermedio de esta red social, más que informarse.
[245] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. Óp. Cit. 46p.

contenidos digitales, tales como videos, fotos, texto, etc., otorgando a los usuarios la posibilidad de interactuar y viralizar el contenido compartido en la red.

- Redes sociales de contenido profesional: destacan Linkedin, Xing y Viadeo. Permiten establecer contactos con otros profesionales, estando dirigidas a un público más especializado y adulto.

Es importante señalar que, si bien cada red social tiene distintos objetivos, todas ellas están sometidas al mismo marco jurídico aplicable a nivel interno e internacional. En efecto, todas las redes sociales son servicios de la sociedad de la información o medios de comunicación social; esto conlleva una serie de consecuencias jurídicas, tanto en el caso español como en el chileno, que será revisado posteriormente.

A continuación, se centrará el análisis en las redes de comunicación o de ocio, en particular Facebook y Twitter.

4. Principales redes sociales de comunicación.

Facebook y Twitter se perfilan como las redes de comunicación con la mayor cantidad de usuarios activos a nivel mundial. Así Facebook durante

el año 2014 registro más de 1 billón de usuarios, mientras que Twitter en segundo lugar, registró 560 millones de usuarios activos.

Ambas cifran han demostrado la importancia que han adquirido este tipo de redes sociales en el diario vivir del usuario, desplazando en muchas ocasiones el uso del correo electrónico como medio de comunicación social, pues el usuario prefiere utilizar las plataformas virtuales ya sea para comunicarse de forma privada con otro usuario o compartir diversos contenidos, la gran mayoría de índole privada, en el ámbito de las redes sociales.

4.1. Facebook.

La red social Facebook (en adelante FB o Facebook, indistintamente) creada por Mark Zuckerberg inició su actividad como plataforma virtual de comunicación en el año 2004, sin embargo, su acceso y uso estaba limitado únicamente a los estudiantes de Harvard. Con el transcurso del tiempo, Facebook empezó a ampliar su espectro a otras universidades, hasta que en el año 2006, se expandió a todo el mundo, siendo en la actualidad la red social con más usuarios.

Facebook permite el acceso a su red condicionado a la entrega por parte de los potenciales usuarios de una serie de datos personales e incluso sensibles, pues su finalidad es construir una verdadera identidad digital del usuario.

Los principales servicios que componen Facebook son los siguientes:

- Perfil: todo usuario que se ha registrado tiene un perfil, el cual es una colección de fotos, historias y experiencias que ha compartido la persona en la plataforma social. El perfil también incluye lo que se denomina biografía, la cual es el espacio por el que se visualizan las publicaciones que el usuario dueño del perfil realiza o en las que se le etiqueta, otorgando FB la posibilidad de configurar la privacidad del perfil y de la biografía.
- La lista de amigos: permite al usuario poder agregar a cualquier persona que esté registrada en la red social, siempre y cuando esta última manifieste su consentimiento, aceptando la invitación de amistad. En la actualidad la lista de amigos ha evolucionado, otorgando al usuario la posibilidad de configurar distintos niveles de amistad, lo cual tiene consecuencias en las restricciones de

privacidad que se aplicarán. Así los "mejores amigos" tendrán un acceso mayor de información, en contraste, con los que tienen la calidad de "conocidos" o "restringidos".

- Grupos y páginas: además, Facebook otorga la posibilidad de interactuar con personas y entidades distintas a las que se encuentran registradas en la lista de amigos, por intermedio de los grupos y de las páginas.

  Los grupos son espacios pensados para que las personas intercambien opiniones acerca de sus intereses comunes, a modo de ejemplo: viajes, programas de televisión, partidos políticos, etcétera. Mientras que las páginas permiten a organizaciones, empresas, famosos y marcas reales comunicarse con la gente a la que gustan, teniendo por finalidad esencial la difusión publicitaria. La creación de las páginas solo se permite a los representantes oficiales o figuras públicas como tal, estableciendo el mecanismo de verificación como medida de seguridad, con el objetivo de evitar la suplantación de identidad.

- Chat: permite enviar mensajes instantáneo a los usuarios que estén registrados en la red social Facebook, teniendo como característica esencial el carácter de privado y, por tanto, restringe el contenido de

comunicación solo respecto a los participantes de dicha comunicación.

Adicionalmente, Facebook destaca por haber dado espacio al desarrollo de aplicaciones, las cuales también pueden ser desarrolladas por terceros, compatibles con Facebook, ofreciendo así un mayor número de servicios y usos en la plataforma. Sin embargo, estas aplicaciones traen consigo mayores amenazas a la privacidad y datos personales de sus usuarios y de la gente que no pertenece a la red social.

En síntesis, Facebook es la red social más popular y utilizada a lo largo de todo el mundo, permitiendo la interconectividad e interacción espontánea entre los usuarios en la red.

4.2. Twitter.

Es un servicio de redes sociales y *microblogging*[246] creado durante el año 2006, que permite al usuario enviar mensajes de texto (tuitear) de una longitud máxima de 140 caracteres mediante página web, mensajería instantánea desde el celular o mensaje de texto. Las actualizaciones se

[246] El microblogging es un servicio que permite a sus usuarios enviar y publicar mensajes breves (alrededor de 140 caracteres), generalmente solo de texto.

muestran en la página perfil del usuario, y aparecen en la página principal de los usuarios que decidieron hacerle *follow* a esta cuenta de Twitter.

Es importante señalar que existe debate respecto a la naturaleza de Twitter, en cuanto a si es una red social o no, ya que su creador, Jack Dorsey, ha llegado a señalar que no es una red social, sino una nueva forma de comunicación[247], fundamentando su postulado al estimar que la esencia de Twitter es la información abierta, destinada a permitir al usuario descubrir las últimas novedades relacionadas con los temas que le interesan.

En el mismo tenor, la AEPD y la Inteco concuerdan en que no es una red social, al señalar que no existe interacción entre sus usuarios, limitándose esta, como máximo, al envío de mensajes de textos y a la actualización de perfiles mediante el uso de fotografías comentadas[248]. Sin embargo, estimo que dichos argumentos no son suficientes como para descartar la naturaleza de red social de esta plataforma virtual.

---

[247] FRÍAS, Álvaro. 2009. Twitter no es una red social, es para todo el mundo sepas qué haces al momento. [en línea] El Mundo en internet. 26 de marzo, 2009. <http://www.elmundo.es/elmundo/2009/03/25/navegante/1237985543.html>[consulta:06 de noviembre de 2015]

[248] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. Óp. Cit. 46p.

En efecto, si bien en Twitter se da en menor medida el elemento de reciprocidad, porque no hay necesidad de seguir a alguien que te está siguiendo, esto no es un motivo suficiente para señalar que no existe interacción social. En este contexto, Jason Fry[249] señala que más que medir el índice de interacción en una plataforma virtual para considerarla como red social, lo primordial es su potencialidad de interacción social, lo que, en nuestra opinión, claramente se da en Twitter, al tener la capacidad de generar conversaciones y *feedback* entre sus usuarios.

Sin embargo, es importante señalar que, al margen del debate respecto a la naturaleza de Twitter, no hay impedimento para que la normativa imperante en privacidad y protección de datos personales le sea aplicada tanto en España como en Chile, lo cual procederemos a analizar en las siguientes líneas.

[249] FRY, Jason. 2010. Why Twitter looks like a social network but feels like new media. [en línea] NiemLab en internet. 7 de mayo, 2010. <http://www.niemanlab.org/2010/05/why-twitter-looks-like-a-social-network-but-feels-like-news-media/>[consulta:06 de noviembre de 2015]

5. Régimen jurídico aplicable a las redes sociales.

La realidad europea a nivel de normativa comunitaria se ha preocupado en adecuar la legislación vigente en materia de protección de datos en el ámbito de las redes sociales; mediante la dictación de una serie de dictámenes y la reforma en tramitación de la Directiva 46/95/CE. Lo cual en conjunto con la labor realizada por España, y en específico su Agencia Española de Protección de Datos, ha fundamentado y reforzado la obligatoriedad de estas plataformas en el respeto y protección de los datos personales de sus ciudadanos. Al contrario, en Latinoamérica, la disparidad en la normativa existente en materia de protección de datos conlleva a que este tipo de plataformas virtuales no adecúe sus servicios a la realidad de nuestro continente.

A continuación, se procederá a analizar la realidad normativa tanto de España como de Chile, con la finalidad de confirmar los postulados anteriormente señalados.

5.1 España.

i) El estándar Bodil Lindqvist.

Para entender cómo se aplica la normativa imperante en materia de privacidad y protección de datos personales en las redes sociales, es primordial hacer referencia al caso Bodil Lindqvist. Este último permitió al Tribunal Constitucional Europeo definir con claridad los criterios para la aplicación de la Directiva 95/46/CE ante el tratamiento de datos personales en una página web.

El Tribunal Sueco tuvo la oportunidad de conocer un proceso penal en contra de Bodil Lindqvist[250], quien fue acusada de haber infringido la normativa sueca relativa a la protección de datos personales, por motivos de publicar en su sitio web diversos datos de carácter personal de varias personas que colaboraban junto a ella en una parroquia.

La página web contenía información de ella y de 18 compañeros más de la parroquia que incluía nombre completo, situación familiar, número de teléfono y hasta información médica, la cual es considerada como dato sensible. El problema central radicó en que la Señora Lidqvist no había informado a sus compañeros de la existencia de esta página web, no solicitó

[250] La Señora Lidqvist era una catequista sueca, que al final de 1998 realizó un curso de informática y con los conocimientos adquiridos creó con su ordenar personal diversas páginas web con la finalidad de que los feligreses de la parroquia que preparaban su confirmación pudieran obtener fácilmente información que pudiera resultarles útil.

el consentimiento previo de sus compañeros y tampoco habría informado a la Datainspektion de la creación de esta página web[251].

En el procedimiento judicial, la Señora Lidqvist reconoció los hechos pero negó que hubiera cometido una infracción y, por tanto, consideraba improcedente pagar una multa a la cual se le condenó, recurriendo de protección en los tribunales superiores suecos.

Ante esta particular situación, el Tribunal Sueco suspendió el procedimiento en segunda instancia, con la finalidad de consultar al Tribunal Constitucional Europeo respecto a la procedencia de aplicar la Directiva 95/46/CE en el presente caso. El Tribunal Constitucional Europeo estimó que la referida directiva era aplicable, aduciendo los siguientes argumentos[252]:

- La directiva se aplica a cualquier tratamiento de datos personales contemplados en el artículo 3, con independencia de los medios utilizados. De esta forma, la Comisión estimó que la difusión de datos personales en internet constituye un tratamiento de datos

[251] Organismo público para la protección de los datos transmitidos por vía informática.
[252] LUXEMBURGO. Unión Europea. 2003. Sentencia del tribunal de justicia C-101/01, noviembre 2003.

personales, en concordancia con la definición otorgada en el artículo 2[253] de la directiva, y, por tanto, se encuentra dentro de su ámbito de aplicación. Asimismo, la Comisión especificó que se trataría de un tratamiento en parte automatizado, pues el hecho de publicar una página web en un servidor, así como realizar operaciones necesarias para hacer accesible a otras personas esta web, son procedimientos de índole técnica, por tanto, automatizadas.

- No se aplica la excepción de vida privada[254]. La Comisión estimó que el tratamiento de datos personales que realizó la Señora Lidqvist no podía inscribirse en el marco de la vida privada, pues, en este caso, existió difusión de dichos datos por internet, resultado accesible un número indeterminado de personas.
- Los conflictos entre el derecho a la protección de datos y la libertad de expresión deben ser resueltos por las autoridades y órganos jurisdiccionales. Sin embargo, la Comisión recuerda que la interpretación jurisprudencial que realicen sus autoridades debe estar

[253] Del concepto de tratamiento otorgado por artículo 3 de la Directiva 95/46/CE, se deriva que la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un tratamiento de esta índole.
[254] COMUNIDAD EUROPEA. Directiva 95/46/CE. artículo 3: "Las disposiciones de la presente directiva no se aplicarán al tratamiento de datos personales efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas."

> en conformidad con la directiva, teniendo la cautela de no generar conflicto con otros derechos fundamentales tutelados por el ordenamiento comunitario o con los otros principios generales del derecho comunitario, como el principio de proporcionalidad.

En conclusión, si bien en aquella época las redes sociales eran impensables, los criterios del Tribunal Constitucional Europeo perfectamente se aplican a estas plataformas virtuales; así lo ha considerado el Grupo de Trabajo del Artículo 29 y diversas autoridades expertas en la materia, destacando la opinión del ex Director de la AEPD, Artemi Rallo, quien señala:

> "Si aplicamos literalmente las conclusiones de este caso a una opinión en el muro de una red social es evidente que, bajo ciertas condiciones, existirá un tratamiento sujeto a la Directiva. Y lo mismo sucederá si se etiqueta una fotografía o se púbica un vídeo que concierna a personas identificas o identificables"[255].

En conclusión, la Directiva 95/46/CE es perfectamente aplicable en el ámbito de las redes sociales, y, no solo a los proveedores de estos servicios,

[255] RALLO, A. y MARTÍNEZ, R. Protección de datos personales y redes sociales: obligaciones para los medios de comunicación. Óp. Cit. 43p.

sino que también al usuario promedio. Por ello, es trascendental educar a la población respecto a los usos indebidos de las redes sociales y sus consecuencias jurídicas.

ii) Recomendaciones del Grupo de Trabajo sobre protección de datos del artículo 29.

El Grupo de Trabajo del artículo 29 (en adelante, GT29) es un organismo de la Unión Europea con carácter consultivo e independiente, creado por el artículo 29 de la Directiva 95/46/CE para la protección de datos y el derecho a la intimidad, el cual está integrado por las autoridades de protección de datos de todos los estados miembros y por el supervisor europeo de protección de datos.

El GT29 por intermedio de sus dictámenes, documentos de trabajo, informes y recomendaciones se ha pronunciado sobre diversas materias relacionadas a la privacidad y protección de datos personales[256]. Si bien las decisiones del GT29 jurídicamente no son vinculantes, como ha señalado la

[256] COMUNIDAD EUROPEA. Dictamen 4/2004: relativo al tratamiento de datos personales mediante vigilancia por videocámara; Dictamen del grupo de trabajo del artículo 29 sobre el tratamiento de datos personales en el contexto laboral; Dictamen 7/2000 sobre propuesta de la Comisión Europea de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y la protección a la intimidad en el sector de las comunicaciones, Opinión 01/2015 y Opinión 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones.

AEPD, tienen un importante valor doctrinal y son frecuentemente utilizados y citados por los tribunales españoles y europeos.

En materia de redes sociales, en concordancia con el razonamiento utilizado en el caso Bodil Liqdvist, se ha de analizar el Dictamen 5/2009[257] sobre las redes sociales en línea. Este tiene por finalidad analizar la aplicabilidad de las directivas comunitarias, en específico la Directiva 95/46/CE y la 98/34/CE modificada por la Directiva 98/48/CE, y, además, realizar una serie de recomendaciones respecto a las obligaciones de los servicios de redes sociales (en adelante, "SRS", indistintamente) y derechos de los usuarios.

En cuanto la aplicabilidad de la Directiva 95/46/CE, el GT29 señala que se aplicará en la mayoría de los casos de proveedores de SRS, aunque su sede se encuentre fuera de los Estados europeos. Asimismo, señala que la Directiva 2002/58/CE sobre privacidad y las comunicaciones electrónicas también se aplicará a los SRS, en cuento a las normas derivadas de las direcciones de IP y la utilización de *cookies.*

[257] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 5/2009 sobre redes sociales en línea. [en línea] <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf> [consulta: 11 noviembre 2015]

El GT29 define como responsable del tratamiento de datos a los proveedores de SRS en virtud de la Directiva 95/46/CE[258] que, como se analizó en el caso Bodil Lidqvist, es aplicable. En efecto, los SRS proporcionan los medios que permiten tratar los datos de los usuarios, así como todos los servicios básicos vinculados a la gestión de los usuarios. Los proveedores de SRS determinan también la manera en que los datos de los usuarios pueden utilizarse con fines publicitarios o comerciales, incluida la publicidad proporcionada por terceros.

Sin embargo, debido a la complejidad de estos servicios de la información, el GT29 también ha calificado como responsables del tratamiento de dato a los proveedores de aplicaciones y, en ciertos casos, a los mismos usuarios.

Por regla general, al usuario común de las redes sociales se le aplica la excepción de vida privada o exención doméstica[259], la cual tiene como

[258] En la actualidad se encuentra una reforma propuesta del nuevo reglamento de 25 de enero 2012.[en línea]<http://www.cgcom.es/sites/default/files/375_prop_reglamento_proteccion_datos.pdf> [consulta: 11 diciembre 2015]. Para mayor información respecto a su análisis y aplicación en las redes sociales consultar TRONCOSO, Antonio. 2013. Las redes sociales a la luz de la propuesta del reglamento general de protección de datos personales. Revista d'Internet, Dret i Política (16):27-39.
[259] COMUNIDAD EUROPEA. Directiva 96/45/CE. artículo 3°.

consecuencia la no aplicación de la Directiva 95/46/CE. Sin embargo, como se analizó en el caso de Bodil Lidqvist, existen ciertos casos donde la exención doméstica no puede cubrir las actividades de un usuario en las redes sociales y, entonces, puede llegar a considerarse que ha asumido algunas obligaciones propias de un responsable de datos y, por tanto, se le aplicaría la Directiva 95/46/CE, bajo ciertas condiciones:

- Cuando el SRS se utiliza como una plataforma de colaboración para una asociación o empresa o se utiliza principalmente como una plataforma con fines comerciales, políticos o sociales[260].
- Tampoco se aplicará la exención doméstica cuando se traten datos de terceros sin su conocimiento y/o consentimiento, particularmente cuando se trate de datos especialmente protegidos.

El GT29 termina haciendo referencia a los derechos de los usuarios de las redes sociales, al establecer que tanto los miembros como los que no forman parte de la red social, pueden ejercer los derechos de los interesados, contenidos en la Directiva 95/46/CE[261], que se traducen en los derechos arcos, ya descritos y analizados tanto en la normativa española

[260] En Facebook, las "páginas" quedarían comprendidas en esta clasificación, mientras que en el caso de Twitter lo serían los perfiles de empresas.
[261] COMUNIDAD EUROPEA. Dictamen 95/46/CE. artículos 10 y 14.

como chilena. Señala el GT29 que los SRS deberán establecer un procedimiento de denuncias de fácil acceso y uso; finalizando con que los usuarios deberían poder tener derecho a adoptar un seudónimo, con el objeto de poder resguardar su identidad digital y, por tanto, reforzar la protección de sus datos personales.

iii) Normativa interna.

En el ámbito de las redes sociales, en primer lugar, deben ser respetados los derechos fundamentales reconocidos tanto a nivel internacional como nacional. De esta forma, los derechos contenidos en el artículo 18 CE, referidos al derecho a la intimidad y derecho a la protección de datos personales deben ser también protegidos en el marco de las redes sociales, resultando imperioso asegurar su eficiencia y eficacia en el sistema.

Para lograr los objetivos anteriormente descritos, es necesaria la dictación de una serie de leyes sectoriales que refuercen y aseguren la debida protección y cumplimiento del derecho a la privacidad y protección de datos personales.

Es relevante mencionar que, desde un punto de vista jurídico, las redes sociales son servicios de la sociedad de la información (en adelante, SSI) y,

por ello, es aplicable con carácter general la normativa contenida en la Ley 32/2002 de servicios de la sociedad de la información y de comercio electrónico.

En efecto, como se describió anteriormente, la referida ley otorga un sentido amplio y general respecto a lo que se debe considerar como servicio de la sociedad de la información, por lo que tienen cabida las redes sociales dentro de su definición. Así, en la exposición de motivos de esta ley, se señala que se considerará por SSI a aquellos proveedores a través de internet que suministren información por dicho medio, al alojamiento en los propios servidores de información, así como cualquier otro servicio que se preste a petición individual de los usuarios siempre que represente una actividad económica para el prestador.

De lo anterior se colige que dentro de la concepción amplia de SSI, concebida por la presente ley, caben las redes sociales. En efecto, los proveedores de redes sociales suministran diversa información por intermedio de su red social con la finalidad de instruir e incluso ofrecer servicios adicionales a sus usuarios; mientras que la petición individual del

usuario al servicio es equiparable al registro y aceptación de las condiciones y políticas de privacidad en la red social.

Asimismo, en la mayoría de los servicios de redes sociales se pueden asociar a la cuenta del usuario, tarjetas de créditos con la finalidad de acceder a ciertos servicios *premium* y/o aplicaciones pagadas; además, es importante recordar que los datos personales otorgados por el usuario a la red social, tienen un valor económico, pues se les considera la moneda de cambio para poder registrarse y participar en las diversas redes sociales, por lo que en un sentido amplio si se dan las condiciones para poder establecer que el proveedor de los SSI desarrolla una actividad económica y, por tanto, se aplica la normativa de la LSSI.

Asimismo, la LSSI señala que se aplicará su normativa a los prestadores de SSI establecidos tanto en algún estado miembro de los Estados europeos como los que no, siempre que el destinatario de los servicios resida en España y se aplicará en todo aquello que no contravenga con los tratados o convenios internacionales. Así en el caso de Facebook y Twitter, que tienen su sede principal en Irlanda[262], Estado miembro de la comunidad Europea,

[262] Si bien ambas entidades son de EE.UU. por motivos económicos y tributarios, tienen sus sedes en Irlanda.

queda comprobado que la LSSI le es aplicable en su totalidad, y, en consecuencia, deben cumplir con las responsabilidades de los prestadores de servicios de alojamiento de datos y aquellos SSI que faciliten enlaces a contenidos o instrumentos de búsqueda, en virtud de lo dispuesto en el artículo 16 y 17 de la referida normativa.

Ahora, si se analiza la normativa existente en función a la materia que trata la presente memoria, he de hacer referencia a la legislación existente en el ámbito de la privacidad[263], es decir, la Ley Orgánica 1/1982 y 15/1999 de protección de datos de carácter personal y el Real Decreto 1720/2007.

En relación a la Ley Orgánica 1/1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, esta normativa no regula de forma expresa las situaciones en específico que pueden llevar a una transgresión de la privacidad en general en las redes sociales. Por ello, es importante asegurar el derecho a la intimidad personal y familiar, en este tipo de plataformas virtuales, mediante la adecuación de la normativa existente frente a las nuevas amenazas y realidades que van surgiendo con el progreso de las TIC.

[263] GIL, Ana. El fenómeno de las redes sociales y los cambios en la vigencia de los Derechos Fundamentales. Óp. Cit. 224p.

Si bien la LSSI reforzó la protección del derecho a la privacidad, mediante una mayor regulación a los proveedores de SSI a través de internet, es necesario implementar medidas adicionales a la normativa. Como ha señalado la AEPD es necesario emprender en desarrollar tecnología jurídica, tomando como base actividades relacionadas con la investigación, el desarrollo y la innovación.[264] Solo de esta forma, debido al carácter dinámico y mutable del derecho a la intimidad, se puede interpretar de forma correcta y armónica los artículos 7 y 8 que establecen los criterios generales que deben ser considerados por la labor jurisprudencial, para responder de cuándo una intromisión será ilegitima en una red social y, por tanto, procederán las sanciones emanadas de la responsabilidad civil.

En último lugar, es importante señalar que con el uso de las redes sociales, el ámbito de la privacidad informacional es el que mayormente se ve vulnerado por el uso de este tipo de plataformas virtuales. En efecto, el deseo del usuario de interactuar con otros le incentiva a compartir en las redes sociales una serie de datos personales, incluso aquellos de índole sensible, construyendo verdaderas identidades digitales, apetecidas por su

[264] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. Óp. Cit. 10p.

valor económico, tanto por los proveedores de redes sociales como por desarrolladores de aplicaciones y terceros.

La Ley Orgánica 15/1999 y su Real Decreto 1720/2007 se aplican en materia de redes sociales porque los proveedores de los servicios de redes sociales, los desarrolladores de aplicaciones y, en ciertos casos, los usuarios son considerados como responsable del fichero de datos y/o encargado del tratamiento, debiendo cumplir en consecuencia con la normativa contenida en la LOPD. Toma especial relevancia en lo que concierne al respeto de los derechos arco que tienen los usuarios de las redes sociales, debiendo, por tanto, otorgar los proveedores de estos servicios diversos mecanismos de denuncias, de fácil acceso para los usuarios, que permitan el adecuado ejercicio de sus derechos arco y los demás reconocidos en la LOPD y el RLOPD[265].

En aquellos casos en los cuales al usuario se le considera responsable o encargado de un fichero, no aplica la excepción de vida privada contenida en el artículo 2 a de la LOPD. La Agencia Española de Protección de Datos con sus resoluciones ha dado respuestas a casos de vulneración de derechos

[265] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 5/2009 sobre redes sociales en línea. Óp. Cit. 14p.

sobre protección de datos, derivados del uso de las redes sociales, otorgando los principales parámetros interpretativos a nivel interno respecto a la adecuación de la normativa existente en el ámbito de las redes sociales.

En consideración a lo anterior, se debe destacar el criterio construido por la AEPD, con la finalidad de comprender en qué casos al usuario se le considera encargado o responsables de ficheros de datos y, por ello, se le aplica la LOPD y el RLOPD. Así, la AEPD señala que para que opere la exención de actividades personales o domésticas estas actividades deben ser propias de una relación personal o familiar. Esto es, equiparable a la que podría realizarse sin la utilización de internet, lo que no sucede en el caso que la publicación se efectué en una página web de libre acceso para cualquier persona o cuando el alto número de personas invitadas a contactar con dicha página resulte indicativo de que dicha actividad se extienda más allá de lo que es propio de dicho ámbito[266].

[266] Así lo establece el Informe 615/2008 de la AEPD [en línea] <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>[consulta: 29 de noviembre 2015]

De lo anterior se desprende que, desde el ámbito de las redes sociales, para llegar a calificar si se aplica la exención de privacidad, se deberá considerar la expectativa de privacidad que tiene el usuario, siendo por tanto necesario analizar el grado de configuración de la publicación, es decir, si está en nivel público o privado, así como el número de amigos o seguidores de la cuenta, con la finalidad de corroborar el número de personas que tienen acceso a esa publicación, y, por tanto, califique como una actividad que se extienda más allá de lo que se considere privado.

5.2. Chile.

i) Recomendaciones de la OCDE.

A nivel de tratados internacionales, a diferencia de la realidad europea y española, la cooperación a nivel continental en materia de privacidad y protección de datos personales se ha desarrollado de forma tardía, existiendo al presente gran disparidad normativa respecto a esta materia. A modo de ejemplo, solo algunos países cuentan con autoridades de control a nivel latinoamericano[267], cumpliendo con ello el estándar adecuado de privacidad exigido por los organismos internacionales, entre ellos la UE.

[267] Argentina, Canadá, Colombia, Costa Rica, Estados Unidos, México, Perú y Uruguay.

En el ámbito de redes sociales, es destacable el informe de la OCDE del año 2002, llamado Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales[268], el cual tiene por afán establecer los estándares mínimos de protección a la privacidad frente a fenómenos tecnológicos como el internet, lo cual es plenamente adaptable a las redes sociales. Así, los principios, descritos en el capítulo II, que inspiran la actual reforma a la Ley 19.628, deben ser respetados tanto por los proveedores, desarrolladores y usuarios en la participación en estas plataformas virtuales.

En las redes sociales, el respeto de estos principios se traduce en el deber de obtener los datos personales con medios legales y justos expresándose esto en condiciones y políticas de privacidad que sean adecuadas, exactas y de fácil entendimiento, para que el consentimiento otorgado por el usuario sea válido. Adicionalmente, el establecimiento de salvaguardias razonables de seguridad para proteger los datos personales contra diversos riesgos. Lo

[268] OCDE. 2002. Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales. [en línea] <http://www.oecd.org/sti/ieconomy/15590267.pdf> [consulta: 29 de noviembre 2015]

anterior; se expresa, a modo de ejemplo, con el establecimiento de una configuración de privacidad máxima por defecto y el reforzamiento de los mecanismos de verificación de la identidad digital. Respecto a lo señalado anteriormente, es importante recordar que presta especial relevancia la edad, ya que a nivel internacional y en la reforma a la Ley 19.628, el consentimiento de los menores de edad exige requisitos adicionales y, por lo tanto, medidas adicionales de seguridad en las plataformas virtuales.

ii) Normativa interna.

A nivel de derechos fundamentales reconocidos por nuestra Constitución Política de la República, el derecho a la vida privada se encuentra consagrado en forma general en el artículo 19 N° 4 y desde su perspectiva material en el N° 5 del mismo artículo. En Chile no está consagrado de forma explícita el derecho a la protección de datos personales a nivel constitucional.

Los Tribunales Superiores de Justicia, a través del recurso de protección, han tenido contadas ocasiones de desarrollar los principales criterios normativos en el ámbito de las redes sociales. Esto es lamentable frente al auge y masificación que han tenido este tipo de plataformas virtuales, más

aun con la masificación del uso de los *smartphones* y tecnología 3G, que permite acceder en cualquier lugar y momento a dichas redes sociales.

La Corte Suprema ha señalado que es legítimo dar de baja a un carabinero por haber publicado en su biografía de Facebook un comentario considerado ofensivo contra un superior[269]. Fundamenta su posición señalando que dicha información fue obtenida por comentarios de terceras personas, por lo que la institución de Carabineros nunca obtuvo acceso a la cuenta, además, señaló que "el actor a través de su red social expone a un número determinado de personas sus comentarios sin que exista prohibición de que aquellos terceros que lo reciben puedan comentarlo con otras personas", por lo que estimo que no se ha vulnerado su derecho a la vida privada.

Esta decisión es lamentable, ya que la Corte Suprema no analizó la expectativa de privacidad del usuario, y, en consecuencia, no tomó en cuenta la configuración de privacidad de su cuenta de Facebook, ni el número de amigos que este tenía. En este sentido, señaló el voto disidente del ministro Muñoz que el consentimiento es un elemento esencial a

[269] CHILE. Corte Suprema. 2012. Figueroa Silva con Prefecto de la Prefectura Cautín, Causa Rol: 5322-2012.

considerar, pues la información y comunicación es pública solo para aquellos a quienes se autorizó expresamente a formar parte de su "lista de amigos" en Facebook, no existiendo habilitación para que dicha información sea utilizada por terceros.

A nuestro juicio, el voto disidente está en lo correcto, porque para determinar si un ámbito de Facebook es público o privado, se debe considerar la expectativa de privacidad del usuario y desde ella desarrollar el criterio jurisprudencial. Así lo efectúa el Tribunal Constitucional español, respecto a estudiar los criterios para aplicar la excepción de vida privada o no.

Una sentencia reciente de la Corte Suprema señala que la publicación de una fotografía en una red social sin el consentimiento de la persona vulnera su derecho a la propia imagen. Esto porque considera que se encuentra implícitamente comprendido como un atributo de la privacidad de la persona y, por tanto, protegido por el artículo 19 N° 4. En este caso la Corte

sancionó al infractor a que tome todas las medidas necesarias para eliminar dicha publicación de la plataforma social[270].

Pese a que esta investigación considera que el derecho a la propia imagen y el derecho a la vida privada son derechos que protegen diversos intereses jurídicos, estimo que el razonamiento de la Corte Suprema fue correcto, pues se compartió la imagen de un tercero sin su autorización expresa, virilizándose públicamente dicha publicación; por lo que, si bien se vulnera el derecho a la propia imagen, también se ha vulnerado el derecho a la vida privada.

Ahora, como fue analizado en el capítulo II, la Ley 19.628 "Sobre protección a la vida privada y datos personales, es la encargada de regular el tratamiento de los datos con carácter personal en registros o bancos de datos tanto de organismos públicos y particulares, con excepción del que se efectúe en el ejercicio de las libertades de emitir opinión e informar, el cual se regula en la Ley 19.733 "Sobre libertades de opinión e información y ejercicio del periodismo".

[270] CHILE. Corte Suprema. 2015. Venegas Yáñez con Álvarez Marchant. Sentencia Rol N° 9.973-2015.

Así, en el ámbito de las redes sociales, al mismo tenor que la normativa española, se considerará como responsable del registro o banco de datos a la persona natural o jurídica privada, o al respectivo organismo público a quien competen las decisiones relacionadas con el tratamiento de los datos de carácter personal. Como bien señala el Consejo para la Transparencia, lo que caracteriza al responsable es su capacidad de decisión respecto de la finalidad, contenido y uso de tratamiento de datos[271]. Así, desde el análisis de este elemento, tanto el proveedor de los servicios red social, los desarrolladores de aplicaciones y, en ciertos casos, los usuarios serán considerados responsables en los términos de esta ley.

Sin embargo, a diferencia de España, en Chile no se han desarrollado los criterios de aplicación de la Ley 19.628 respecto al usuario común ya que nuestra normativa no reconoce alguna excepción de vida privada, y por tanto, desde este punto de vista, no presenta problemas para su aplicación. Sin perjuicio de que, para la generalidad de los casos, el usuario común es

[271] CONSEJO PARA LA TRANSPARENCIA. Recomendaciones sobre protección de datos personales por órganos de la Administración del Estado. [en línea] <http://www.cplt.cl/transparencia_activa/mecanismos/propuesta_de_recomendacion_pd_general_version_consulta_publica_11abril2011.pdf> [consulta: 29 de noviembre 2015]

considerado titular de los datos y, por tanto, titular para ejercer los derechos arco, pese a que no existen mecanismos de coerción y prevención efectivos para cautelar los datos personales de los usuarios en las redes sociales.

Un tema trascendental en el ámbito de las redes sociales es definir la fuente accesible al público, lo cual puede conllevar a ciertas confusiones en el ámbito de las redes sociales.

La ley ha definido como fuente accesible al público los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes[272]. Ciertamente es un concepto amplio, pero deficiente, ya que la normativa establece que no se requerirá el consentimiento en aquellos casos en que el tratamiento de datos personales provenga o se recolecten de fuentes accesible público. La ley no regula, respecto al origen de los datos, su legitimidad; pudiendo interpretarse, en consecuencia, que el solo hecho de ser de acceso público legitimaría el tratamiento de los datos, sin el consentimiento de su titular[273], lo que

[272] CHILE. Ley 19.628. artículo 2 letra i.
[273] La reforma detalla de mejor forma esta definición, siendo muy parecida a la de España pero sin hacer referencia al origen de estos datos motivo por el cual los problemas persiste. En ese sentido ver, DERECHOSDIGITALES. Minuta de discusión sobre Boletín 8.143-03 [en línea] <https://www.derechosdigitales.org/wp-content/uploads/comentariosdd-datos.pdf> [consulta: 29 de noviembre 2015]

conlleva reconocer una serie de irregularidades, tales como, evitar el cumplimiento del principio de confidencialidad de los datos, la finalidad del tratamiento, entre otras.

Así, por ejemplo, si un usuario en las redes sociales tiene un deficiente grado de configuración de privacidad, gran cantidad de amigos y su cuenta de la red social está indexada a un motor de búsqueda, podría llegar a considerarse que dicho perfil es una fuente accesible al público y, por tanto, no necesitaría el consentimiento expreso de su titular para que un tercero pueda recopilar y tratar dichos datos, sin importar si el origen de dicha información es legítimo.

Especialmente problemático resulta que en la mayoría de las redes sociales el grado por defecto de privacidad es bajo y la opción de indexar el perfil a los principales motores de búsquedas está por defecto autorizada. Ello aumenta el riesgo de llegar a considerar un perfil como de fuente accesible al público y, en consecuencia, los datos de ese usuario podrían ser recopilados y tratados por terceros sin su consentimiento expreso.

España, a diferencia de Chile, tuvo cautela en la regulación de las fuentes accesibles al público, estableciendo un listado taxativo y

adicionando una serie de condiciones para que dicho tratamiento sin el consentimiento de su titular fuera legítimo en los términos de la LOPD y RLOPD[274]. Además la AEPD ha colaborado en el esclarecimiento de lo que se debe considerar por fuente de acceso público[275], llegando a la conclusión de que internet y las redes sociales no son fuentes accesibles al público, por no estar en la enumeración taxativa contenida en la LOPD, requiriendo por tanto el consentimiento inequívoco del usuario para la recopilación y tratamiento de sus datos.

En síntesis, si bien se ha apuntado a describir ciertos temores respecto a la aplicación de la normativa en las redes sociales, no hay duda de que las redes sociales, los desarrolladores de aplicaciones y en ciertos casos los usuarios deben respetar la normativa contenida en la Ley 19.628, sin perjuicio de que, a diferencia de la normativa española[276], Chile no señala de forma explícita el ámbito de aplicación de la Ley 19.628. No obstante, y

[274] ESPAÑA. LOPD. artículo 6.
[275] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 0342/2008 [en línea] <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2008-0342_Recabar-datos-de-p-aa-ginas-web-c--no-constituye-un-tratamiento-basado-en-fuentes-accesibles-al-p-uu-blico.pdf>[consulta: 29 de noviembre 2015]
[276] ESPAÑA. LOPD. artículo 2.

en concordancia con los tratados internacionales suscritos y ratificados por Chile, el reconocimiento del derecho fundamental a la vida privada y el principio general de la buena fe, estimo que los proveedores, desarrolladores de aplicaciones y usuarios, que se encuentren dentro y fuera del territorio chileno, deben respetar y cumplir con esta normativa en cuanto a la obtención del consentimiento, recolección y tratamiento de datos, y, también, al asegurar el ejercicio de sus derechos arco a los usuarios de estas plataformas. Para efectos de reforzar la protección de la privacidad en el ámbito de internet es necesario tener claridad respecto a cuáles serán las bases de datos que se tendrán como fuentes de acceso público y las razones de por qué se permitirá esto. Como señala Alvarado, Chile debiese seguir el modelo español ya que este considera "la aplicación de un catálogo cerrado de bancos que puedan considerarse fuentes de acceso público a datos personales, de modo tal que la excepción quede limitada y que el consentimiento por parte del titular de los datos mantenga su fuerza de regla general[277]."

[277] ALVARADO, Francisco. 2014. Las fuentes de acceso público a datos personales. Revista de derecho y tecnología. 3(2):205-226.

Para finalizar, se hará referencia a la Ley 19.733 "Sobre libertades de información y opinión y el ejercicio del periodismo", pues tiene importantes consecuencias en el ámbito de las redes sociales.

En primer lugar, las redes sociales serían un tipo de medio de comunicación social de acuerdo a la definición otorgada por la ley.[278] En efecto, estas plataformas virtuales ofrecen la posibilidad de interacción mediante la transmisión, divulgación, difusión y/o propagación de forma estable y periódica de textos, sonidos o imágenes destinados al público, cualquiera sea el soporte o instrumento utilizado.

En relación a lo anterior, hay que destacar que la generalidad de los medios de comunicación tradicionales han creado un perfil en las diversas redes sociales, con la finalidad de llegar a un mayor número de personas y poder interactuar con el público, publicando a lo menos cuatro días en cada semana, además de existir otros tantos que solo cuentan con un perfil en la red social para divulgar la información. Con la aprobación de la reforma, estos serían considerados un diario digital o electrónico y, en consecuencia,

[278] El artículo 2 de la Ley 19.733 establece que, para todos los efectos legales, son medios de comunicación social "aquellos aptos para transmitir, divulgar, difundir o propagar, en forma estable y periódica, cualquiera sea el soporte o instrumento utilizado."

deben cumplir con la normativa contenida en la presente ley, además de asegurar el derecho a acceso y rectificación al presunto afectado u ofendido también en el ámbito de las redes sociales.

En segundo lugar, la Ley 19.733 reconoce el derecho de toda persona natural o jurídica de fundar, editar, establecer, operar y mantener medios de comunicación social, sin otras limitaciones que las señaladas en la ley. De lo anterior se desprende el reconocimiento explícito a favor de toda persona natural o jurídica de emitir opinión e informar sin censura previa en las plataformas de redes sociales, sin perjuicio de responder de los delitos y abuso que se cometan en conformidad a la ley.

En tercer lugar, en el caso de aprobarse la reforma en tramitación (contenida en los boletines 9460-19 y 9461-19[279]), la cual busca actualizar la actual normativa y hacerle extensiva a los medios digitales, cabe mencionar que esta ha generado una serie de controversias respecto a si las cuentas de las redes sociales de los usuarios comunes que publiquen a lo

[279] Para más información sobre las reformas en trámite, consultar: [en línea] <https://www.camara.cl/> [consulta: 29 de noviembre de 2015]

menos cuatro días en cada semana deberán cumplir con los requisitos exigidos a los diarios[280].

Sin embargo, el diputado Farías[281] señaló que dicha interpretación de la reforma era errónea, pues lo que se pretende es entregar una mayor regulación a los diarios electrónicos y no coartar la libertad de expresión, señalando que la reforma en tramitación no regularía las redes sociales. Aun así, la definición de medio de comunicación social es aplicable en el ámbito de las redes sociales, siendo necesario especificar y delimitar los efectivos alcances de esta ley en caso de aprobarse la comentada reforma.

6. Principales amenazas contra la privacidad y datos personales en las redes sociales.

La tecnología es neutral, pero su utilización no lo es. Como señala Drummond, el problema surge cuando aquellos que pueden utilizar la tecnología de modo eficiente y más productivo no lo hacen con

[280] Requisitos contenidos en el título III de la Ley 19.733.
[281] Diputado Farías y proyecto de diarios digitales: "No busca cobrar por uso de redes sociales ni coartar la libertad de expresión. [en línea] Cámara de Diputados de Chile. 6 de enero, 2015. https://www.camara.cl/prensa/noticias_detalle.aspx?prmid=124852> [consulta: 29 de noviembre de 2015]

neutralidad[282]. Así, con el vertiginoso avance de las TIC han surgido nuevas amenazas, impensables en décadas anteriores, contra la privacidad y los datos personales.

Las redes sociales otorgan una serie de beneficios a la sociedad porque permiten la interconectividad e interacción simultánea con personas ubicadas en diversas partes del mundo, además del ejercicio del derecho a la libertad de opinión e información por intermedio de estas plataformas. Aun así, en el otro lado de la moneda, implican trasgresiones y amenazas a la privacidad de las personas y, en específico, la recolección y tratamiento indebido de los datos personales vertidos las redes sociales.

Lo anterior implicó que la preocupación a nivel internacional por el uso de estas plataformas virtuales haya aumentado, elaborándose al respecto diversos informes, directrices y recomendaciones dirigidas tanto a los proveedores de estas plataformas, desarrolladores de aplicaciones web y a los usuarios de las redes sociales. Esta reacción ha sido dirigida a reforzar la seguridad de la privacidad de los datos y fortalecer los mecanismos de protección, especialmente respecto los grupos más vulnerables como los

[282] DRUMMOND, Víctor. Internet, Privacidad y Datos personales. Óp. Cit. 27p.

menores de edad e incapaces frente a las innumerables amenazas que se originan por la sobreexposición de la identidad digital en este tipo de plataformas virtuales.

6.1. Expectativa de privacidad.

En el último tiempo se ha originado la discusión respecto a si es plausible que el usuario de redes sociales tenga o no una legítima y razonable expectativa de privacidad[283] en este tipo de plataformas virtuales.

Aquellos que estiman que no es plausible tener una expectativa de privacidad en las redes sociales, lo hacen argumentando que internet es una red abierta y, como tal, es de libre acceso a todos, por tanto, es un error considerar tener una expectativa de privacidad en un espacio considerado como público[284]. A mayor abundamiento, señalan que es el usuario quien decide sobreexponer de forma voluntaria su vida privada, teniendo como

[283] Concepto desarrollado en EE.UU. utilizado por la jurisprudencia norteamericana con la finalidad de evaluar los límites de la privacidad en cada caso en concreto. Para mayor información consultar: SALDAÑA, María. 2001. El derecho a la privacidad en los Estados Unidos: Aproximación diacrónica a los intereses constitucionales en juego. Revista Teoría y realidad constitucional (28):279-312.

[284] AREYUNA, Héctor. 2014. Espionaje web: "Tener expectativa de privacidad en internet es un error". [en línea] Diario Uchile en internet. 30 de enero, 2014. <http://radio.uchile.cl/2014/01/30/espionaje-web-tener-la-expectativa-de-privacidad-en-internet-es-un-error>[consulta: 29 de noviembre de 2015]

consecuencia la complejidad de controlar la recolección y tratamiento de datos en este tipo de plataformas[285].

Sin embargo, considerar que internet sea de libre acceso y sin mayores restricciones; no significa que las personas no puedan tener espacios donde puedan apartarse de la observación ajena. En efecto, como bien señala Novoa Monreal, no todo lo que se dice en un espacio público es de contenido público; así las conversaciones personalizadas se consideran privadas por motivos de ser consideradas una manifestación de un pensamiento que generalmente está dirigido a un destinatario determinado[286]. Estimo que el mismo razonamiento, puede ser aplicado en el ámbito de las redes sociales, siendo por tanto plausible que el usuario tenga una expectativa de privacidad en ellas. En efecto, el usuario de este tipo de plataformas también tiene una expectativa de privacidad la cual varía dependiendo de una serie de elementos tales como, cantidad de amigos, configuración de privacidad del perfil, entre otros. La expectativa será mayor en aquellos casos donde el usuario opte por comunicarse

[285] En las redes sociales no hay ninguna expectativa de tener privacidad. [en línea] El Diario Montañés en internet. 19 de febrero, 2015. <http://www.eldiariomontanes.es/sociedad/201502/19/redes-sociales-ninguna-expectativa-20150219003559-v.html>[consulta: 29 de noviembre de 2015]

[286] NOVOA M., Eduardo. Derecho a la vida privada y Libertad de Información. Óp. Cit. 203p.

mediante *inbox* en Facebook o *direct messages* en Twitter, pues para todos los efectos serán consideradas comunicaciones privadas ya que son realizadas a usuarios determinados y consta la intención de mantener dicho espacio al resguardo de la observación ajena. En caso contrario el usuario podría haber elegido otro medio de comunicación en la red social ya sea mediante publicación de un mensaje en un muro o enviar un tuit público, según corresponda.

La expectativa de privacidad es fundamental desde el punto de vista jurisprudencial, ya que al momento de evaluar los límites de la protección al derecho a la vida privada la judicatura debe considerar y analizar la expectativa de privacidad del usuario en el ámbito de las redes sociales. Reafirmando lo anterior, señala Rayman Labrin: "Cuando entregamos información personal en las redes sociales, esa información sigue siendo privada mientras tengamos la expectativa de que esa información no será utilizada por terceros"[287].

En consecuencia, la expectativa de privacidad del usuario es subjetiva, variando de usuario en usuario. No obstante, la expectativa de privacidad

[287] RAYMAN, Danny. 2015.Vigilancia y derecho a la privacidad en internet. Revista Chilena de Derecho y Tecnología 4(1):187-232.

objetiva es aquella legítima y plausible, la cual es considerada y analizada por la judicatura ante un caso de posible transgresión al derecho a la privacidad. Para tales efectos, creo que los elementos a considerar en el ámbito de las redes sociales con el efecto de discernir si la expectativa de privacidad del usuario es legítima y plausible serán los siguientes:

- Configuración de privacidad de la cuenta:

No cabe duda que, tanto desde la perspectiva de la normativa chilena como de la española, las comunicaciones vertidas por *inbox* en Facebook o mensaje directo en Twitter son consideradas comunicaciones privadas, independiente del contenido de la comunicación. Lo anterior se fundamenta en la posibilidad que estos servicios otorgan de personalizar el envío de mensajes a destinatarios específicos, quedando, en consecuencia, amparadas dichas comunicaciones por el derecho fundamental a la privacidad.

Ahora, el conflicto surge con los contenidos publicados en la biografía de Facebook o en el perfil[288] de Twitter, pues dependerá de la configuración

[288] Tu perfil muestra la información que eliges compartir públicamente, como así también todos los Tweets que publicas. Tu perfil y tu @nombredeusuario sirven para identificarte en Twitter. Conforme establecen sus políticas. TWITTER. 2015. Centro de ayuda. [en línea] <https://support.twitter.com/articles/352810> [consulta: 29 de noviembre 2015]

de privacidad que haya seleccionado el usuario, para evaluar su expectativa de privacidad.

En el caso de Facebook se ofrece la opción de configurar la privacidad de la cuenta del usuario[289], lo cual permite administrar las preferencias de privacidad básicas, tales como: quién puede ver las publicaciones, así como activar el registro de actividad[290]. En consecuencia, dependiendo del nivel de configuración de privacidad de la cuenta se colige el grado de expectativa de privacidad que este considera tener. Así, mientras mayores son las restricciones de acceso al contenido compartido, mayor es la expectativa de privacidad del usuario en la red.

Mientras que en Twitter, por su parte, la expectativa de privacidad dependerá de si la cuenta es pública o está protegida. Así, en las cuentas protegidas, el grado de expectativa del usuario es mayor, pues este debe

[289] Así, Facebook ofrece varias opciones de configuración de privacidad, desde el público, es la configuración por defecto, hasta por amigos, o personalizados, debiendo otorgar los nombres en específico de quienes pueden ver este contenido. FACEBOOK. 2015. Políticas de privacidad. [en línea] <https://www.facebook.com/help/325807937506242> [consulta: 29 de noviembre 2015]

[290] El registro de actividad en Facebook otorga al usuario la posibilidad de revisar todas las publicaciones y contenidos en los que se le etiquete por terceras personas. Así, si niega su autorización, no se podrá asociar su cuenta de Facebook a tal contenido; sin perjuicio de que los amigos de la persona en cuestión podrán seguir viéndolo, sin embargo, se puede solicitar por otras vías la eliminación del contenido, ya sea denunciando en caso que procediera ante Facebook, o enviando un mensaje al que público el contenido pidiéndole que lo elimine.

aprobar de manera manual a todas y cada una de las personas que pudieran ver los tuits de dicha cuenta; otorgando, en consecuencia, un mayor control respecto a quienes pueden ver la información contenida en ese perfil, así como la imposibilidad de retuitear el contenido de dicha cuenta.

A diferencia de Facebook que, exige a sus usuarios la utilización de sus verdaderos nombres, Twitter otorga la posibilidad de ocupar un seudónimo. Este es otro elemento a considerar para establecer si existe una expectativa de privacidad legítima y plausible, pues mediante el uso de un seudónimo los usuarios pueden enmascarar su verdadera identidad.

- Cantidad de amigos o seguidores:

La cantidad de amigos en Facebook o seguidores en Twitter es otro factor determinante a tener en cuenta. En efecto, a mayor número de contactos, mayor es la probabilidad de que se virilice determinado contenido en la red y, por tanto, desde un punto de vista objetivo, menor será la expectativa de privacidad del usuario.

- Indexación del perfil en el motor de búsqueda:

Los buscadores de internet recopilan y tratan los datos personales derivados del uso de servicio de las redes sociales. Así, si una persona

escribe el nombre de otra en el buscador, automáticamente puede aparecer la cuenta de perfil que este tiene asociada en determinada red social. Lo anterior permite a terceros a acceder al contenido público que esta persona comparte en la red social, también la posibilidad de seguirlo o agregarlo a la lista de amigo. Lo anterior demuestra que, desde un punto de vista objetivo, la expectativa de privacidad de este usuario es menor a la que tiene un usuario que optó por no indexar su perfil a un buscador de internet.

6.2. Principales riesgos.

Los mayores riesgos contra la privacidad y los datos personales, se producen en las redes sociales catalogadas de ocio, tales como Facebook y Twitter.

La necesidad de interacción del usuario conlleva a que este sobreexponga su vida privada en la red, desconociendo los ataques malintencionados que terceros pueden realizar en base a esta información, así como la ignorancia de las condiciones y políticas de privacidad contenidas en estos servicios, careciendo, por tanto, de un efectivo conocimiento de cómo se recopilarán y con qué finalidades se tratarán sus datos personales.

Dentro de este contexto, la AEPD en coordinación con la INTECO, en el año 2008, publicó un estudio titulado *Sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*[291]. Este ha sido base para desarrollar los principales criterios sobre la aplicabilidad de la normativa de privacidad y datos personales en el ámbito de las redes sociales, analizando, para tales efectos, los principales riesgos y amenazas presentes en ellas.

Dentro de este contexto, procederemos a describir y analizar las principales amenazas a la privacidad y datos personales, utilizando para tales efectos la clasificación realizada por la AEPD y la Inteco, quienes reconocen tres momentos críticos: el registro, la participación del usuario en la plataforma, y la decisión de darse de baja en la red social.

6.2.1. Registro.

[291] Dicho estudio tuvo por afán concientizar al usuario respecto a los contenidos que comparte en estas plataformas virtuales, así como realizar una serie de recomendaciones a los proveedores de los servicios de las redes sociales y los desarrolladores de aplicaciones, con la finalidad de reforzar la protección a la privacidad y datos personales en este tipo de plataformas virtuales. [en línea] <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/estudio_inteco_aped_120209_redes_sociales.pdf>[consulta: 29 de noviembre 2015]

El usuario promedio de las redes sociales no tiene conciencia de la naturaleza de los datos que vierte en el formulario de registro, así como del valor que estos pueden alcanzar en el mercado. Vale la pena que reiteremos que los servicios de redes sociales no son gratis, a pesar de que los proveedores señalen lo contrario[292] induciendo al error a los usuarios.

El peso de las redes sociales en el mercado es proporcional al grado de intimidad que los usuarios revelan en sus conexiones. Es en el registro donde los proveedores de estos servicios tienen la oportunidad de recabar gran cantidad de datos de carácter personal y sensible, resguardando su actuar en políticas y condiciones de privacidad poco claras y de excesivo contenido, configurando así un contrato de adhesión por el cual el usuario se ve obligado a aceptar todas y cada una de sus condiciones para poder acceder a estos servicios.

Como consecuencia de lo anterior, la propia red social impone una serie de obstáculos al usuario con la finalidad de obtener la mayor cantidad de datos de este, además de obtener amplias libertades para su tratamiento, lo

[292] Facebook encabeza el formulario de registro con la frase "Registrarte es gratis y lo será siempre".

que se traduce en una serie de situaciones que exponen la vida privada y datos personales del usuario.

i) El tipo de datos solicitados en el registro, aunque no sean obligatorios, son excesivos.

Como bien señala el informe de la AEPD y la Inteco[293], con frecuencia las redes sociales solicitan a los usuarios datos relativos a su ideología política, religiosa y sexual. Si bien son datos de carácter voluntario, el usuario desconoce las implicancias que conlleva la entrega de este tipo de datos, para su vida y las personas de su entorno.

Los datos concernientes a ideología política, preferencia religiosa y sexual desde un punto de vista normativo son considerados datos especialmente protegidos o datos sensibles, respecto a los cuales la normativa exige requisitos especiales para su recolección y tratamiento.

Así, el artículo 7 de la LOPD señala que nadie podrá ser obligado a declarar sobre su ideología, religión o creencia y, en caso que desee hacerlo, deberá otorgar su consentimiento expreso y por escrito. Al mismo tenor, el

[293] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. Óp. Cit. 110p

Dictamen 5/2009 señala que si un servicio de red social incluye en el formulario de registro preguntas relativas a datos sensibles, deberá indicar muy claramente que la respuesta a tales pregunta es totalmente voluntaria.

En el caso de Facebook estos requisitos no son cumplidos a cabalidad, ya que la plataforma en ningún momento advierte al usuario del derecho que este tiene a no declararlos, así como tampoco tiene la diligencia de obtener el consentimiento expreso y por escrito del usuario; solo lo insta a completar el formulario sin dar mayores detalles al respecto, además de otorgarle a este tipo de datos una configuración por defecto casi pública[294].

En consecuencia de lo anterior, ante la excesiva cantidad de datos de carácter personal y sensibles solicitados por la red social, sumado a la ignorancia del usuario promedio respecto a las implicancias que conlleva el compartirlos, los ataques informáticos han aumentado con la intención de recabar de forma maliciosa esta gran base de datos, destacando el *pishing* como mecanismo informático para acceder de forma fraudulenta a ellos.

En el ámbito de las redes sociales, el *pishing* consiste en la creación de sitios web falsos con la apariencia de la página de inicio de la red social, las

[294] Configuración: Amigos de mis amigos.

cuales tienen por finalidad inducir por engaño al usuario a registrarse e identificarse en ellas, recabando automáticamente sus datos personales para ser utilizados de forma indebida. Ya sea suplantando la identidad del usuario, exponiendo la vida privada de este, robando el número de tarjetas bancarias asociadas a la red social y, en general, confeccionar verdaderas bases de datos con la finalidad de venderlas a terceros.

Así, en el año 2013 en Twitter fueron robadas más de 250.000 cuentas, con sus claves, correos y otros datos[295]. Mientras que Facebook es la red social que más ataques de *pishing* ha recibido según un estudio publicado por la empresa informática Kaspersky.[296]

En consecuencia, mientras mayor sea la cantidad de datos vertidos en la red social, mayores serán las consecuencias negativas contra la privacidad de los usuarios a causa de los ciberataques y el tratamiento indebido de sus datos.

[295] Robadas 250.000 cuentas de Twitter. [en línea] El País en Internet. 4 de febrero, 2014. <http://tecnologia.elpais.com/tecnologia/2013/02/04/actualidad/1359967398_800973.html>[consulta: 29 de noviembre de 2015]
[296] DEMIDOVA, Nadezhda. 2014. Social network frauds. [en línea] Securelist en internet. 11 de junio, 2014. <https://securelist.com/analysis/publications/63855/social-network-frauds/>[consulta: 29 de noviembre de 2015]

Algunos usuarios con la intención de poder participar en este tipo de plataformas crean perfiles falsos con la finalidad de preservar su privacidad, sin embargo, las mismas condiciones de uso de estas plataformas, obligan al potencial usuario a entregar datos personales reales, prohibiendo de forma explícita la creación de cuentas falsas, instando a la comunidad en general de esta red social a denunciar todas las cuentas falsas, a pesar de aquellas que no tengan por motivo suplantar la identidad de otra persona o hacer un uso indebido en la red social. Lo anterior es contrario a la recomendación realizada tanto por la AEPD, Inteco e incluso el GT29, quienes sugieren a los servicios de redes sociales la posibilidad de otorgar a sus usuarios el derecho de poder utilizar un seudónimo y así poder resguardar su identidad digital[297].

ii) La problemática del consentimiento y las condiciones de uso abusivas.

La manifestación de consentimiento es un elemento esencial para perfeccionar el contrato de adhesión[298] entre el usuario y la red social. En el caso de Facebook y Twitter ambas señalan que el consentimiento del

[297] En Twitter esto sí se respeta.

[298] Es un contrato de adhesión por lo que el contenido de las cláusulas es establecidas por una parte de forma unilateral, la red social, en consecuencia el usuario no puede alterar el contenido de las cláusulas, debiendo aceptar la totalidad de ellas en el contrato.

potencial usuario se concreta al momento que este hace clic en el botón de registro y con ello acepta sus condiciones de uso. Sin embargo, en el ámbito de las redes sociales, muy pocos leen las condiciones de uso o, si lo hacen, no las entienden y, por ende, la mayoría desconoce cómo se tratan sus datos, qué obligaciones tiene el proveedor de los servicios de redes sociales y desarrolladores de aplicaciones, así como qué derechos tienen los usuarios.

De esta forma, como bien señala la AEPD, a pesar de que las condiciones de uso están recogidas en el sitio web, no alcanzan su finalidad última: que el usuario comprenda el objeto, la finalidad y el plazo para el que son recabados y tratados sus datos personales[299]. Lo anterior, en palabras de Daniel Solove[300], se debe a dos problemas centrales que presenta la manifestación del consentimiento en el ámbito de internet. En primer lugar, el usuario es desinformado y carece de interés por leer las condiciones de privacidad al ser largas y difíciles de comprender. En consecuencia, las personas entregan rutinariamente sus datos a cambio de

[299] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. Óp. Cit. 110p

[300] SOLOVE, Daniel. 2013. La autogestión de la privacidad y el dilema del consentimiento. Revista chilena de derecho y tecnología. 2(2):11-47.

beneficios bastantes menores ya que no dan gran valor a su privacidad. En segundo lugar, si bien existen personas racionales e informadas que valoran su privacidad esto no es suficiente, pues las entidades que recolectan, utilizan y dan a conocer los datos de una persona son demasiadas, careciendo la persona promedio de tiempo necesario para administrar su privacidad en todas las entidades que tienen sus datos y, además, está el problema de fiscalizar el cumplimiento de las finalidades por las cuales se otorgó el derecho a recolectar y tratar dichos datos.

De tal forma, surge el siguiente debate, el ordenamiento jurídico debe coartar la capacidad de las personas en dar su consentimiento en ciertas situaciones consideradas peligrosas o se debe confiar en la autogestión de la privacidad, sin analizar el fondo de dicha decisión, respecto a si es buena o mala, centrando su atención en la libertad y voluntad del usuario. En España y demás estados miembros de la UE, han optado por la primera alternativa al exigir una serie de requisitos esenciales que deben estar presentes en toda manifestación de consentimiento para ser considerado válido desde un punto de vista legal.

De acuerdo a la normativa contenida en la LOPD[301], el consentimiento del usuario de la red social deberá ser libre, inequívoco, específico e informado. Siguiendo a José Miguel Beltrán[302], el consentimiento será libre cuando sea otorgado al margen de cualquier presión o coacción, debiendo evitarse todo tipo de violencia, intimidación o error, mientras que el consentimiento será inequívoco cuando se preste sin dejar lugar a duda o equivocación. El consentimiento será informado cuando los proveedores de los servicios de redes sociales suministren la información de forma clara y sencilla, puesto que gran cantidad de usuarios son menores de edad[303]. Además, los menores de 14 años[304] deberán contar con el consentimiento de sus padres o tutores para el uso de una red social. Y para finalizar, el consentimiento será específico cuando el usuario de la red social manifiesta su voluntad con una finalidad determinada y explícita. En consecuencia, para que este elemento sea respetado, los proveedores de servicios de redes sociales y los desarrolladores de aplicaciones deberán estipular de forma

[301] En Chile, la actual reforma a la Ley 19.628 pretende consagrar el consentimiento en los mismos términos señalados en la normativa española contenida en la LOPD.

[302] BELTRÁN, José. 2014. Aproximación al régimen jurídico de las redes sociales. Cuaderno Electrónico de Estudios (2): 61-90.

[303] Lo anterior en directa concordancia con la normativa contenida en la RLOPD, que además dispone como requisito adicional, que para recabar datos de cualquier menor de 14 años es necesario el consentimiento de los padres y tutores.

[304] En otros lugares del mundo la edad mínima para poder hacer uso de este tipo de plataformas virtuales es de 13 años.

específica y detallada para qué fines utilizaran sus datos, quienes tendrán acceso a ellos y la utilización de datos sensibles[305].

Asimismo, el GT29 en su Dictamen 15/2011 sobre la definición del consentimiento[306] señala que, en el ámbito de las redes sociales, el carácter específico del consentimiento también significará que si los fines para los que los datos son tratados por el responsable cambian en algún momento, el usuario deberá ser informado y estar en condiciones de dar su consentimiento para el nuevo tratamiento de datos, debiendo comunicársele las consecuencias del rechazo.

Sin embargo, estimo que el cumplimiento de los requisitos del consentimiento en el ámbito de las redes sociales es complejo, por una serie de razones:

- La expectativa de privacidad que tiene el usuario no se condice con lo estipulado en las condiciones de uso.

[305] Grupo de Trabajo sobre Protección de Datos del Artículo 29. Dictamen 15/2011 sobre la definición del consentimiento. [en línea] <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_es.pdf> [consulta: 29 de noviembre 2015]
[306] Ibíd. 21p.

- La mayoría de los usuarios no leen las condiciones de uso[307].
- La generalidad de las condiciones de uso constan de un excesivo lenguaje técnico y gran cantidad de páginas.
- Al ser un contrato de adhesión impuesto por la red social al usuario las condiciones de usos consta de cláusulas generales, sin mayor especificación respecto a los distintos fines para los que trataran los datos personales de sus usuarios. Lo anterior es una grave amenaza a la privacidad y datos personales de los usuarios en la red, pues induce a una serie de prácticas abusivas por parte de estas plataformas con la intención de maximizar el uso de los datos, expandiendo los fines para lo cual se recopilaron estos datos.

Para finalizar, el GT29[308] ha mencionado que la simple pulsación de un botón no puede considerarse consentimiento válido para el tratamiento de datos personales, ya que el consentimiento no puede consistir en una autorización en términos generales.

---

[307] Para demostrar la ineficacia del sistema actual, la empresa PC Pitsop estipuló en sus términos y condiciones de uso que daría 1.000 de dólares al primero que los leyera. Pasaron cuatro meses antes de que un usuario reclamara el premio. [en línea] <http://www.pcpitstop.com/spycheck/eula.asp> [consulta: 29 de noviembre 2015]

[308] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes. [en línea] <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_es.pdf> [consulta: 29 de noviembre 2015]

En conclusión, ante las diversas problemáticas que presenta la manifestación del consentimiento en el ámbito de las redes sociales, si bien es loable la intención de resguardar la privacidad de las personas desde la perspectiva legal al establecer una serie de requisitos que debe cumplir el consentimiento, es además necesario educar al usuario de las redes sociales en cuanto a la verdadera importancia de la privacidad desde un punto de vista económico y social.

A continuación procederé a analizar de forma somera, puesto que excede el ámbito de esta memoria, las principales amenazas a la privacidad que se pueden desprender de las condiciones de uso de Facebook y Twitter.

En el caso de Facebook, destacan las siguientes cláusulas:

> "Recopilamos el contenido y otros datos que proporcionas cuando usas nuestros Servicios, por ejemplo, al abrir una cuenta, al crear o compartir contenido, y al *enviar mensajes o al comunicarte con otras personas*. La información puede corresponder a datos incluidos en el contenido que proporcionas o relacionados a este".

De lo anterior se desprende que los mensajes enviados por *inbox* también son recopilados, aun cuando estos tengan la naturaleza de conversaciones privadas.

Asimismo, como comprobó el australiano Max Schrems[309], Facebook también guarda el registro de las conversaciones privadas eliminadas, lo cual es realizado sin el conocimiento del usuario, viéndose en consecuencia imposibilitado a ejercer su derecho de cancelación.

Lo anterior no es de extrañar, pues hemos de recordar que ya en el año 2009 quedaron expuestos una serie de mensajes privados en las biografías de sus usuarios[310].

> "Las empresas pertenecientes a Facebook o administradas por Facebook nos proporcionan información sobre ti, de acuerdo con sus respectivas condiciones y políticas".

A modo de ejemplo, una de las empresas pertenecientes a Facebook, que en la actualidad cuenta con más de 80 millones de usuarios en el mundo, es

[309] El ciudadano austriaco Max Schrems interpuso una denuncia en Irlanda contra Facebook, porque consideraba que la empresa no garantizaba la seguridad de sus datos.
[310] JIMÉNEZ, Rosa. 2012. Facebook deja al descubierto mensajes privados. [en línea] El País en internet. 25 de septiembre, 2012. http://tecnologia.elpais.com/tecnologia/2012/09/24/actualidad/1348507026_917653.html [consulta: 29 de noviembre de 2015]

WhatsApp. En virtud de lo señalado por esta cláusula, se desprende que los datos vertidos en esta aplicación también pueden ser recopilados por Facebook.

Lo cual ha preocupado a varios sectores[311], porque nadie asegura que Facebook no recopile de forma indebida las conversaciones privadas de los usuarios de WhatsApp con la finalidad de utilizar los datos recabados con fines publicitarios o de otra índole.

Y para finalizar Facebook señala: "Si no cumpliéramos alguna parte de esta Declaración, no se considerará una exención".

Ciertamente es alarmante esta cláusula pues deja al usuario en indefensión, sin ninguna garantía de exigir a Facebook que cumpla con las condiciones y políticas de privacidad, ya que si Facebook no cumple alguna de las cláusulas el contrato no queda invalidado[312].

[311] Facebook espía tus conversaciones de WhatsApp, según Avast, [en línea] ABC Tecnología en internet. 30 de octubre, 2015. <http://www.abc.es/tecnologia/redes/abci-whatsapp-facebook-espia-conversaciones-whatsapp-segun-avast-201510301733_noticia.html> [consulta: 29 de noviembre de 2015]

[312] Facebook: estas son las condiciones que aceptas sin leer. [en línea] 24Horas en internet. 11 de febrero, 2014. http://www.24horas.cl/tendencias/tecnologia/facebook-estas-son-las-condiciones-que-aceptas-sin-leer-1071759> [consulta: 29 de noviembre de 2015]

En cuanto a las condiciones de uso de Twitter, hemos de destacar la siguiente cláusula:

> "Si ha compartido información, como mensajes directos o *tweets* protegidos, con otro usuario que acceda a los servicios de Twitter a través de un servicio de terceros, tenga en cuenta que la información se puede compartir con el servicio de terceros".

Si bien esta cláusula tiene por finalidad informar al usuario de posibles riesgos a su privacidad, es importante hacer mención a ella. Pues en síntesis la plataforma virtual reconoce que aun cuando el usuario tenga la configuración máxima de privacidad, es decir sus tuits protegidos, existe la posibilidad que servicios de terceros accedan a ellos y puedan verse expuesto los datos del usuario con fines maliciosos o desconocidos.

iii) Grado de configuración por defecto del perfil.

Como adelantamos, en la etapa de registro se otorga la oportunidad al usuario de configurar debidamente el grado de publicidad de su perfil, de tal forma que determine desde el comienzo quiénes podrán tener acceso a la información que publique y comparta.

Sin embargo, gran cantidad de los usuarios de estas redes sociales desconoce las diversas consecuencias que conlleva el exponer su vida privada y otros datos relativos a su personalidad de forma pública en las redes sociales. Por este motivo diversas entidades, expertas en la materia, han recomendado a los proveedores de estos servicios la implementación de una configuración por defecto privada. De esta forma, si el usuario decide compartir contenido de forma pública, este deberá personalizar su configuración, constando por este acto su consentimiento inequívoco. Ya que, el optar por un grado de configuración pública del perfil, conlleva una serie de consecuencias que en la generalidad de los casos no son previstas por el usuario promedio.

El GT29 señala que "si no existe ninguna restricción a tal acceso, los terceros podrán acceder a toda clase de detalles íntimos sobre los usuarios, bien como miembros del servicio de red social, o mediante motores de búsquedas"[313], al mismo tenor la AEPD y la Inteco señalan que "la no configuración o la configuración incorrecta de este aspecto puede afectar no solo a los contenidos propios que hubiera publicado, sino también al resto

[313] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 5/2009 sobre redes sociales en línea. Óp. Cit. 7p.

de los usuarios con los que hubiera publicado información compartida, puesto que será accesible por parte del resto de los miembros de la plataforma"[314].

En consecuencia, no solo está en peligro la privacidad del usuario titular de la cuenta pública, sino que, además, la privacidad de los demás usuarios que interactúan con él, así como terceros ajenos a la red social[315].

En concordancia con lo anterior, los principales riesgos que conlleva una configuración pública del perfil son los siguientes:

- Cuando el usuario publica contenido o información en las redes sociales de forma pública[316] permite que todos, incluidas las personas que son ajenas a la plataforma, accedan a dicha información, la utilicen con fines desconocidos.

[314] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. Óp. Cit. 44p.

[315] En algunos casos, las personas con las que te comunicas y compartes información pueden descargar o compartir a su vez este contenido con otras personas tanto dentro de nuestros servicios como fuera de ellos. Cuando haces un comentario en la publicación de otra persona o indicas que te gusta su contenido en Facebook, esa persona decide qué destinatarios pueden ver tu comentario o Me gusta. Si elige la configuración de privacidad "Público", tu comentario será público.

[316] Configuración pública Facebook o no tener Twitter protegido.

- Los motores de búsquedas y otros terceros pueden mantener copias de la información recabada, incluso después de haber sido eliminada dicha información en la plataforma virtual.
- Al exponer los comentarios vertidos de la red social a un mayor número de personas, mayores son las repercusiones que estos tienen en el ámbito social[317].

En consecuencia, si bien se insta a los servicios de redes sociales a optimizar el estándar por defecto a privado, como bien señala la AEPD, la educación del usuario sobre los diferentes aspectos de configuración del perfil y las ventajas de una adecuada restricción en la difusión de datos personales, es el principal mecanismo de protección[318].

6.2.2. Participación del usuario.

[317] Por ejemplo Ximena Ossandón que en ese tiempo era vicepresidenta de la Junji, la cual declaró en su Twitter, que los sueldos eran "reguleques", causando revuelo en la red social y en el entorno nacional, por lo que se vio obligada a renunciar.
[318] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. Óp. Cit. 176p.

i) Publicación excesiva personal y de terceros.

El usuario promedio de las redes sociales con el afán de interactuar comparte una serie de contenidos de índole privado, tales como: comentarios, fotografías, videos, compartir su ubicación, entre otros. Con ello, sobreexpone de tal forma su vida privada que hace posible la construcción de una verdadera bitácora, disponible para un gran número de personas. Aun cuando el grado de configuración de la cuenta ayuda, en cierta forma, a controlar el acceso a dicha información, esto no impide la viralización del contenido por parte de terceros. Por ello, el usuario debe ser cauteloso con el contenido que comparte en la red social, pues puede publicar información que involucra a terceros, sean usuarios o ajenos a la red social.

En este sentido, la AEPD ha señalado que no se puede publicar información y datos de terceros si no han autorizado expresamente su publicación, pudiendo solicitar su retirada de forma inmediata[319]. Por ello, la publicación de datos personales por el usuario de una red social supone la asunción de la responsabilidad ante las personas cuyos datos o fotografías

[319] Ibíd. 8p.

aparecen publicados en el perfil. Es decir, queda obligando al cumplimiento de los principios de la información y el consentimiento.

De esta forma, no solo los proveedores y desarrolladores de aplicaciones pueden ser considerados responsables del tratamiento de datos, sino que también el usuario común.

Aun cuando no se puede censurar de forma previa el derecho de información y opinión, el tercero interesado puede hacer valer contra el usuario que publicó contenido concerniente a él los derechos arco. Pudiendo solicitar, a modo de ejemplo, la eliminación o modificación de un comentario, e incluso la cancelación u oposición, lo que se traduciría en "dejar de ser amigos" o en el "*unfollow*" según sea el caso[320].

ii) Instalación y uso de *cookies* sin el consentimiento del usuario.

Las *cookies*[321] permiten a los proveedores de servicios de red social ofrecer al usuario mecanismos que faciliten su navegación en el sitio así como la posibilidad de personalizar la publicidad que visualizará en su perfil. Para lograr estos objetivos las *cookies* rastrean automáticamente los

[320] RALLO, A. y MARTÍNEZ, R. 2011.Protección de datos personales y redes sociales: obligaciones para los medios de comunicación. Quaderns del CAC 37, 14(2): 41-52.
[321] Término informático relacionado con la información que guarda un servidor sobre un usuario en su equipo.

hábitos de navegación del usuario, recabando una serie de datos que generalmente son de índole personal y, por tanto, exigirían recabar el consentimiento informado del usuario.

Las *cookies* permiten obtener la IP del usuario, y esta es considerada por la AEPD[322] un dato de carácter personal. Lo anterior añadido a otros datos recopilados a través de las *cookies* permite aplicando la teoría de los mosaicos, construir la identidad digital de una persona, exponiendo en consecuencia la vida privada de las personas.

De este modo, es primordial informar al usuario del uso de las *cookies* y contar con el consentimiento previo de este para poder tratar los datos obtenidos de las *cookies* no exceptuadas[323].

En el ámbito de las redes sociales, el usuario manifiesta su consentimiento al momento de registrarse en la plataforma virtual, sin embargo, es difícil desprender de dicho acto el consentimiento inequívoco

[322] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. Óp. Cit. 112p.

[323] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29: Dictamen 4/2012 sobre la exención del requisito de consentimiento de cookies [en línea] <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_es.pdf> Algunas cookies exceptuadas, son: de entrada del usuario, de identificación de sesión de usuario, de seguridad, personalización interfaz del usuario.

del usuario, especialmente considerando las cláusulas de uso generales con la finalidad de maximizar el tratamiento de los datos personales de sus usuarios que utilizan los proveedores.

A modo de ejemplo, Facebook señala en sus condiciones de usos que utiliza *cookies* con la finalidad de realizar análisis y estudios con el fin de mejor sus productos. Señala, además, que puede compartir estos datos con otras empresas socias de la red social, sin especificar en sus condiciones el plazo por el cual estarán activadas.

En virtud de estas condiciones de usos, Facebook justificó la realización de un experimento en el año 2012[324], en el cual manipuló el contenido que aparecía en el *timeline* del usuario, sin el conocimiento de este, con la finalidad de monitorear sus reacciones emocionales, esto constituye una clara transgresión a la privacidad del usuario.

De esta forma el usuario no solo tiene que ser consciente del contenido y datos que comparte de forma explícita en las redes sociales, sino que

[324] AGUIRRE, Francisco. 2014. Facebook "manipula" emociones de casi 700 mil usuarios y desata la polémica. [en línea] La Tercera en internet. 30 de junio, 2014. <http://www.latercera.com/noticia/tendencias/2014/06/659-584708-9-facebook-manipula-emociones-de-casi-700-mil-usuarios-y-desata-la-polemica.shtml>[consulta: 29 de noviembre de 2015]

también debe ser cauteloso con sus acciones implícitas, puesto que los "Me gusta" de Facebook y de Twitter son monitoreados por *cookies*.

iii) Indexación automática en los buscadores de internet.

Como mencionamos, las redes sociales establecen una configuración por defecto que otorga el máximo de publicidad de los datos del usuario, de tal forma que la indexación automática de los perfiles de los usuarios de las redes sociales a los buscadores de internet está por defecto "activada".

En consecuencia, desde que el usuario se registra y participa en la red social sus datos están siendo procesados y publicitados por los buscadores de internet, sin el consentimiento inequívoco del usuario y afectando, además, al principio de calidad de los datos.

La única opción que ofrecen las redes sociales para detener la indexación automática de los perfiles en los motores de búsqueda es que el usuario acceda a su configuración y desactive la opción por defecto. Lo que, por cierto, no desactiva la indexación de forma inmediata, pues las redes sociales señalan que este proceso puede llevar cierto tiempo, y, en consecuencia, terceros podrán seguir accediendo al perfil del usuario desde el buscador de internet.

Asimismo, existe la posibilidad que dichos datos no sean eliminados de la base de datos del motor de búsqueda y, por tanto, sigan expuesto a terceros. Lo cual es un aspecto que en muchas ocasiones el usuario ignora de este hecho, por lo que existe una clara transgresión tanto al derecho de acceso, como al derecho de cancelación que tiene el usuario.

Como señala la AEPD, en su Declaración sobre buscadores de internet[325], el grave peligro de la indexación por defecto automática de los perfiles a los motores de búsqueda consiste en que el tratamiento de dicha información puede permitir registrar las actividades que el usuario lleva a cabo en la red, posibilitando configurar perfiles de este que pueden ser utilizados por la empresa sin que el usuario sea consciente ni esté suficientemente informado.

iv) Aplicaciones sincronizadas a las redes sociales.

En el ámbito de las redes sociales, diversas son las aplicaciones[326] que interactúan con este tipo de plataformas, permitiendo sincronizar el perfil de

[325] Agencia Española de Protección de Datos. Declaración sobre buscadores de internet. [Disponible en:https://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/declaracion_aepd_buscadores.pdf], 2007.

[326] Grupo de Trabajo sobre Protección de Datos del Artículo 29: Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, óp. cit. Considera que son

la red social con una aplicación determinada y viceversa. Esto puede generar una serie de riesgos a la privacidad, que se acrecientan cuando el acceso a la aplicación se efectúa a través de un *smartphone*, porque se puede acceder a otro tipo de información de índole personal, tales como: la lista de contactos contenida en el dispositivo móvil, localización GPS, registros de llamadas, entre otras.

En efecto, como señala el GT29, las aplicaciones pueden recoger grandes cantidades de datos a partir de los dispositivos y procesarlos para proporcionar servicios nuevos e innovadores al usuario. No obstante, esas mismas fuentes de datos pueden ser objeto de un tratamiento adicional, normalmente para generar ingresos, que resultan desconocidas o no deseadas por el usuario final.

De esta forma, los principales riesgos están asociados a una falta de transparencia y conocimiento del tipo de tratamiento que las aplicaciones pueden realizar sobre los datos, esto adicionado a la falta de consentimiento real del usuario antes que se produzca el tratamiento de tales datos.

---

programas informáticos generalmente concebidos para un cometido concreto y dirigido a un determinado conjunto de dispositivos inteligentes.

En relación con lo anterior, es relevante considerar que no todos los desarrolladores de aplicaciones cuentan con condiciones de usos y políticas de privacidad o no informan a sus posibles usuarios de forma clara sobre el tipo de datos personales que recabara la aplicación.

A mayor abundamiento, las redes sociales señalan que, ante la discrepancia de las condiciones de usos, prevalecerán las condiciones de uso de la aplicación, lo cual aumenta el peligro de un tratamiento de datos indebido, pues es más complejo fiscalizar una aplicación que una red social.

En consecuencia, el usuario también debe ser cuidadoso respecto a las aplicaciones que instala en sus dispositivos, ya que también expone los datos contenidos en su red social. A modo de ejemplo, diversas aplicaciones han llegado a robar contraseñas de Facebook y en consecuencia han quedado expuestos a terceros todos los datos contenidos en sus cuentas[327].

6.2.3. Cancelación de la cuenta.

[327] PAGLIERY, José. 2015. Dos juegos para Android roban contraseñas de Facebook. [en línea] CNN en internet. 9 de julio, 2015. <http://cnnespanol.cnn.com/2015/07/09/dos-juegos-para-android-roban-contrasenas-de-facebook/#0>[consulta: 29 de noviembre de 2015]

En ciertas redes sociales, como ocurre en el caso de Facebook, pese a que el usuario solicita dar de baja el servicio conforme a las políticas de privacidad, es imposible cancelar de forma efectiva la cuenta, manteniéndose por tanto a disposición de las redes sociales y de terceros los datos personales del usuario. Por tanto, todo tratamiento que se siga realizando después de esta solicitud es indebido, además de no haber respetado el derecho a cancelación del usuario.

Un riesgo similar se presenta durante la participación del usuario en la red social, porque existe incertidumbre respecto a si el contenido que ha borrado el usuario de su perfil efectivamente es eliminado de las bases de datos de estas plataformas.

En relación a esta problemática, conmoción causó la denuncia realizada por Max Schreems contra Facebook, quien solicitó a la red social copia de todos los datos que tenían almacenados de su perfil, recibiendo para su sorpresa un archivo que contenía información eliminada por él, tales como solicitudes de amistades rechazadas, comentarios eliminados de la biografía, fotografías en las que había sido etiquetado y, posteriormente, eliminó la etiqueta, entre otros. Estimando, en consecuencia, que Facebook

no garantizaba la seguridad de sus datos, por lo que interpone una denuncia ante el Comisionado de Protección de Datos de Irlanda.

Es importante destacar la resolución de este caso, pues la sentencia del Tribunal Europeo repercute directamente en las facultades de las autoridades de control europeas en el ámbito de las redes sociales.

En efecto, la denuncia de Schreems sirvió de argumento para que el Tribunal Europeo señalara que EE. UU., y en consecuencia Facebook, no garantizaba la protección de los datos de los ciudadanos europeos, solicitando por ello a la Comisión Europea que invalidara la normativa que consideraba a EE. UU. como un territorio seguro para la intimidad[328]. Además, señaló que a pesar de que un tercer país sea considerado con un estándar adecuado de privacidad y, por tanto, se permita la transferencia internacional de datos, al tenor de lo dispuesto en la Directiva 95/46/CE, no hay excusa para dejar sin efecto ni limitar las facultades que disponen las autoridades de control respecto a apreciar con total independencia si efectivamente un país cumple con la transferencia de datos.

[328] UNIÓN EUROPEA. Tribunal de Justicia. Comunicado de prensan N°117/15 [en línea] <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf> [consulta: 29 de noviembre de 2015]

En consecuencia, este fallo es trascendental pues reafirma la independencia de las autoridades de control y refuerza las facultades de inspección que estas tienen sobre las redes sociales. Así, las redes sociales ya no se podrán excusar arguyendo que tienen la certificación de puerto seguro de la UE y que cuentan con un estándar adecuado de privacidad. Ahora estarán obligadas a implementar medidas efectivas que reflejen su intención de asegurar la privacidad de los datos de sus usuarios, porque las autoridades de control podrán bloquear la transferencia internacional de datos de cualquier tercer país que, en su opinión, no cumpla con dicho estándar a pesar de contar con la certificación.

Como se ha visto, en el presente capítulo, el desarrollo de la Web 2.0 conllevó un cambio de perspectiva en el uso de internet, transformando al usuario común de internet en el principal generador de contenido, fenómeno que se acrecentó con el surgimiento y posterior masificación de las redes sociales.

Las redes sociales de ocio, como Facebook y Twitter, centran su objetivo en otorgar al usuario de estas plataformas la posibilidad de interactuar y compartir diversos contenidos. Sin embargo, lo anterior implica que el

usuario sobreexponga su vida privada y sus datos personales, sin que sea consciente de los diversos riesgos que conlleva el compartir gran cantidad de datos en las redes sociales.

Ante este nuevo escenario, la UE, y en específico España, han desarrollado diversos criterios con el afán de adecuar la normativa imperante en esta materia en el ámbito de las plataformas virtuales. Así, ha destacado la aplicación del estándar Bodil Lindqvist y las principales consideraciones del GT29, las cuales han permitido a España, y en específico a la AEPD, a adecuar la legislación de protección de datos en este ámbito; y en consecuencia, evitar la desprotección del ciudadano español en las plataformas virtuales.

Muy diferente es la realidad de Chile. Ante la disparidad de normativa a nivel continental y el precario desarrollo de la legislación imperante en el ámbito de internet, y en específico en las redes sociales, resulta complejo adecuar la interpretación de la actual normativa en este aspecto, lo que sumado a la ausencia de una autoridad de control independiente y especializada, hace que la legislación nacional haya perdido eficiencia y eficacia.

VI. ANÁLISIS DE LOS PRINCIPALES REQUERIMIENTOS Y RESOLUCIONES EMANADOS DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN HACIA LAS REDES SOCIALES.

España, a través de su Agencia de Protección de Datos, ha realizado una serie de requerimientos y recomendaciones a las redes sociales, con el afán de que respeten el derecho la intimidad y datos personales de sus ciudadanos, instándolos a adecuar sus condiciones de uso y política privacidad, así como a reforzar la seguridad de los datos personales de sus usuarios, en concordancia con la normativa de la UE y la de España.

Como se ha señalado, ante el vertiginoso avance de las tecnologías surgen nuevas amenazas contra la privacidad, siendo las redes sociales uno de los ejes principales para perpetrar ataques informáticos, recolección y usos indebidos de datos, entre otros. De tal forma, la normativa imperante en la materia corre el riesgo de caer en la obsolescencia, si no se adecúa su interpretación a la realidad actual.

La Agencia Española de Protección de Datos por intermedio de sus resoluciones emanadas tanto del procedimiento de tutela de derechos y

procedimiento sancionador, ha interpretado los principios y normativa vigentes en materia de privacidad y datos personales, con la finalidad de otorgar eficacia y eficiencia al ordenamiento jurídico, resolviendo los diversos conflictos originados por el uso de estas plataformas virtuales.

1. Principales recomendaciones y requerimientos de la AEPD a las redes sociales.

En Europa han comprendido que las autoridades de control, como entidades independientes y especializadas, no solo han de proteger el derecho a la privacidad de los datos personales mediante el ejercicio de sus potestades fiscalizadoras y sancionadoras, sino que también han de ejercer de forma preeminente la potestad de prevención. Lo anterior con el afán de proteger ex ante a los ciudadanos por medio de la difusión y educación, dirigida a los proveedores de los servicios de redes sociales, desarrolladores de aplicaciones y usuarios sobre los derechos, obligaciones y principales desafíos en la protección de datos.

Así lo ha entendido el GT29 mediante la dictación de una serie de Dictámenes relacionados sobre la materia; y, del mismo modo, lo ha

entendido la Agencia Española de Protección de Datos mediante la publicación de informes, estudios y su memoria anual.

En efecto, la AEPD ha participado en diversas iniciativas tendientes a asegurar la privacidad de los datos en el ámbito de internet, en específico en las redes sociales. Destacan para tales efectos el "Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online", el derecho fundamental a la protección de datos: guía para el ciudadano, guía sobre el uso de las *cookies* y una serie de guías orientadas a los menores de edad, ya que son considerados el grupo de mayor vulnerabilidad a los riesgos provocados con el uso de las redes sociales[329].

En conclusión, a grandes rasgos, los diversos estudios, informes y memorias anuales tienen por finalidad:

- Instar a los proveedores de los servicios de redes sociales a una mayor transparencia y facilidad de acceso a la información. Así como a garantizar a los usuarios el control absoluto del tratamiento de sus

[329] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guías destinadas a la protección de usuarios. [en línea] <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php> [consulta: 29 de noviembre de 2015]

datos e información publicada en la red, pues solo de esta forma se pueden garantizar al usuario de las redes sociales el ejercicio de sus derechos arco.

- Fomentar la concientización del usuario común, con énfasis en los usuarios menores de edad, respecto a la seguridad de los datos en las redes sociales, así como dar a conocer los principales peligros a los que se ven expuestos en este tipo de plataformas; como una medida tendiente a aminorar la transgresión a este derecho.
- Describir y analizar los diversos elementos que debe tener el consentimiento otorgado por el usuario, tanto para el uso de las redes sociales, instalación y uso de *cookies*, indexación de datos en los motores de búsqueda, entre otros, con el fin de que la recolección y tratamiento de datos se realice conforme a la normativa comunitaria e interna relativa a la privacidad y protección de datos personales.
- Informar a nivel comunitario e interno de los próximos desafíos a superar en materia de privacidad y protección de datos, a través de la publicación obligatoria en conformidad del artículo 37 de la LOPD de su memoria anual, destacando en el último tiempo la preocupación

de la AEPD por el uso de los *smartphones* como dispositivos de acceso a las redes sociales[330].

A mayor abundamiento, para reforzar las medidas anteriormente mencionadas, la AEPD ha establecido comunicación directa con diversas redes sociales, con el fin de instarlos a respetar la normativa española en materia de privacidad y protección de datos personales.

De esta forma, la Agencia haciendo uso de su potestad de prevención requirió en el año 2009[331] a la plataforma virtual Facebook, para que informara respecto a las medidas de seguridad que adoptaría para proteger la privacidad de los datos de los ciudadanos españoles. En forma concreta, solicitó la mejora en la política informativa de Facebook y de los sistemas de información que se ofrecen a los usuarios, así como la necesidad de establecimiento de mecanismos de verificación de la edad, que permita limitar el acceso de forma efectiva de los menores de 14 años.

[330] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Memoria 2014. [en línea] <http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2014/Memoria_AEPD_2014.pdf> [consulta: 29 de noviembre de 2015]

[331] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. La AEPD traslada a Facebook sus inquietudes sobre los riesgos para la privacidad. [en línea] <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2009/notas_prensa/common/marzo/260309_AEPD_redessociales_facebook.pdf> [consulta: 29 de noviembre de 2015]

Recomendando adicionalmente la posibilidad de establecer una configuración por defecto del máximo grado de privacidad a los usuarios para minimizar los riesgos para la privacidad y los derechos de los usuarios.

Con posterioridad a este requerimiento, Facebook evacuó traslado a la AEPD realizando una serie de modificaciones tendientes a reforzar la privacidad de los datos de sus usuarios; de tal forma implementó el sistema que permite a los usuarios seleccionar con quién comparten la información cada vez que la publiquen y obligó, además, a todos sus usuarios a revisar y actualizar sus configuraciones de privacidad[332].

Sin embargo, el requerimiento de mayor trascendencia en este ámbito, aceptado por Facebook, es la adecuación a la legislación española la edad mínima de sus usuarios[333]. Pues el artículo 13 del RLOPD señala que la edad mínima para que un menor pueda manifestar su consentimiento para el tratamiento de sus datos es desde los catorce años.

[332] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Facebook presenta a la AEPD nuevo sistema que mejorará la privacidad. [en línea] <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2009/notas_prensa/common/julio/200709_Facebook_AEPD_nuevo_sistema.pdf> [consulta: 29 de noviembre de 2015]

[333] Ibíd.

En consecuencia, Facebook incrementó la edad mínima para que los menores que se encuentren en territorio español puedan participar como usuarios de la red social, pues a nivel mundial la edad mínima exigida es de 13 años, en concordancia con la normativa estadounidense, y edad exigida por defecto también en Chile.

Lo anterior demuestra la importancia de la AEPD en el ámbito de las redes sociales, ya que las empresas multinacionales de internet pueden adaptar sus servicios a las exigencias legales nacionales en garantía de la privacidad, en la medida que las autoridades de control de cada país mantengan una relación de colaboración y respeto con este tipo de entidades, así como una rigurosa normativa a nivel comunitario para instar de forma efectiva a que las redes sociales cumplan con el estándar adecuado de privacidad.

2. Principales resoluciones de la AEPD en el ámbito de las redes sociales.

Con el afán de demostrar cómo la Agencia Española de Protección de Datos ejerce de forma eficiente y efectiva sus potestades en el ámbito de las redes sociales, he analizado una serie de resoluciones correspondientes a los

años 2010 al 2015[334], para así dar a conocer los principales criterios considerados por la AEPD al momento de resolver un procedimiento de tutela de derechos o procedimiento sancionador, según sea el caso.

2.1. Resoluciones tutelares de derechos.

Como estudió en el capítulo IV, el procedimiento de tutela de derechos tiene lugar cuando al interesado o afectado se le ha denegado por parte del responsable o encargado del fichero, de forma total o parcial, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación. También si se ha incumplido el deber de información, estipulado en el artículo 25.5 de la RLOPD, esto es, no se ha dado respuesta de su solicitud al afectado, con independencia de que figuren o no datos personales del afectado en sus ficheros.

En el ámbito de las redes sociales las solicitudes a la AEPD para que inicie el procedimiento de tutela de derechos han aumentado[335] debido a que

[334] Para acceder a los diversos procedimientos sancionadores y de tutela de derechos substanciados ante la Agencia Española de Protección de Datos, diríjase a consultar [en línea] <http://www.agpd.es/portalwebAGPD/resoluciones/index-ides-idphp.php>[consulta: 24 de enero de 2016]

[335] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Ejercicio de derechos. [en línea] <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/ejercicio_derechos/index-ides-idphp.php> [consulta: 29 de noviembre de 2015]

el ciudadano español está cada día mejor instruido respecto al ejercicio de sus derechos arco; y que, además, ha adquirido consciencia de la importancia de la protección de sus datos en internet[336].

Del análisis de las resoluciones emanadas por la AEPD en el periodo correspondiente del 2010 al 2015, el 91% de las reclamaciones fueron interpuestas por la denegación del derecho a cancelación en los términos del artículo 16 de la LOPD, es decir, contra aquellos datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente ley y, en particular, cuando tales datos resulten inexacto o incompletos.

Por otro lado, el 9% de las reclamaciones restantes fueron interpuestas por la denegación del derecho a acceso en los términos del artículo 15 de la LOPD[337]. Dicho porcentaje es lógico, pues los usuarios de las redes sociales y terceros ajenos a estas, en la generalidad de los casos, carecen de información respecto a quién, cómo y qué datos están siendo tratados,

[336] Esta encuesta revela que el 86% de los adultos españoles están preocupados por el manejo que hacen las empresas en Internet con su información personal. COMRES. Big brother watch - Privacidad en internet. [en línea] <http://www.facua.org/es/documentos/encuestaprivacidad_esp.pdf> [consulta: 29 de noviembre de 2015]

[337] El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

dificultándose en consecuencia el derecho de acceso. Por el contrario, el derecho de cancelación es el más incoado, ya que se ejerce sobre algo respecto a lo que se tiene cierto conocimiento.

Como bien señala la AEPD, el principio de deber de información "es a la vez más que una obligación para los responsables de los tratamientos, un derecho de los titulares de los datos y, muchas veces, constituye la primera ayuda que tiene el ciudadano para poder ejercitar el resto de derechos que marca la Ley (Acceso, Rectificación, Cancelación y Oposición)"[338].

En el ámbito de las redes sociales, el derecho de acceso se traduce en la posibilidad que tienen los usuarios y terceros ajenos a la red social de descargar una copia de la información contenida en la plataforma virtual. Los usuarios de la plataforma podrán descargar de forma automática la copia de sus datos, mientras que los terceros ajenos a la red social deberán rellenar un formulario realizando la correspondiente solicitud.

Adicionalmente, en el caso que sea un usuario común de la red social quien esté tratando los datos de otra persona sin que sea aplicable la

[338] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Deber de información. [en línea] https://www.agpd.es/portalwebAGPD/canalresponsable/obligaciones/deber_informacion/index-ides-idphp.php] [consulta: 15 de noviembre de 2015]

excepción doméstica, se le podrá solicitar directamente que remita la información que contiene del afectado. Artemi Rallo señala que dicho requerimiento se cumplirá "con ofrecer a quien ejerza el derecho, los pantallazos en los que se muestre a qué datos se accede"[339].

Mientras que el derecho de cancelación se traduce en la posibilidad que otorgan estos servicios de eliminar la cuenta de la red social, eliminar el contenido que publiquen en ella, y, en el caso que se desee ejercer el derecho de cancelación respecto a un usuario de la red social, bastará con dejar de ser amigos o hacerle *unfollow* –según sea el caso–, derecho que podrá ser concretado por ambas partes[340].

Ahora, desde el punto de vista de las plataformas virtuales, el 91% de las reclamaciones involucraba el uso de la plataforma social Facebook, mientras que el 9% implicaba el uso de Twitter. Estimo que esta diferencia porcentual se debe, por una parte, a que la cantidad de usuarios activos en Facebook es aproximadamente el doble a la cantidad de usuarios activos

[339] RALLO, A. y MARTÍNEZ, R. Protección de datos personales y redes sociales: obligaciones para los medios de comunicación. Óp. Cit. 46p.
[340] Ibíd. 46p.

que en Twitter[341]; y, por otra, las características de los servicios de Facebook permiten compartir un mayor volumen de contenido en comparación a la red social de *microblogging*.

Además, es menester señalar que de la totalidad de los procedimientos de tutela de derechos que conoció la AEPD, el 43% de ellos fueron resueltos, mientras que el 57% tuvieron que ser desestimados por la Agencia.

La AEPD desestimó la generalidad de estos procedimientos por motivos de no cumplir con lo consagrado en el artículo 25 de la RLOPD, esto es, no acreditar el derecho a cancelación o acceso ante el responsable o encargado del fichero, "por ello no puede entenderse que se haya ejercido en la forma legalmente establecida el derecho del que se pretenda la tutela de esta Agencia, al ser el ejercicio del derecho requisito previo necesario para poder iniciar dicho procedimiento"[342]. Sin perjuicio de lo anterior, la AEPD

[341] Facebook reporta mil millones de usuarios activos. Cada día la comunidad comparte en total 2,5 mil millones de piezas de contenidos. BENNET, Shea. 2014. Pinterest, Twitter, Facebook, Instagram, Google+, Linkedin Social Media Stats [INFOGRAPHIC].[en línea] http://www.adweek.com/socialtimes/social-media-stats-2014/495727?red=at> [consulta: 29 de noviembre de 2015]

[342] ESPAÑA. AEPD. Procedimiento de tutela de derechos N° TD 815/2012, TD 2047/2012 y TD 2086/2012.

otorga otra oportunidad al afectado, apercibiéndolo para que acredite el ejercicio del correspondiente derecho ante el responsable o encargado del fichero en un plazo de diez días, en virtud de lo establecido en el artículo 71.1 de la Ley 13/1992 de "Régimen jurídico de las administraciones públicas y del procedimiento administrativo común", ley que se aplica de forma supletoria[343].

Lo anterior ciertamente es lógico, pues, a mayor abundamiento, ha señalado la AEPD: "El escrito de solicitud del ejercicio del derecho que se pretende realizar no debe dirigirse a esta Agencia Española de Protección de Datos, ya que esta no tiene los datos personales que se contienen en el fichero de datos, respecto al cual se pretende ejercer el derecho a cancelación"[344].

En estas situaciones, la AEPD luego de desestimar la solicitud, insta al interesado a dirigir a la empresa u organismo responsable su solicitud de acceso o cancelación según sea el caso y, en caso de que se le deniegue o no

[343] ESPAÑA. AEPD. Procedimiento de tutela de derechos N° TD 1558/2012.
[344] ESPAÑA. AEPD. Procedimiento de tutela de derechos N° TD 2047/2012 y N° TD 1912/2013.

se le responda a su solicitud, proceda a realizar nuevamente la reclamación de tutela de derechos ante la Agencia.

Se debe señalar que la AEPD ha estimado que el envío de un mensaje privado al responsable del fichero, sin que se haya acreditado la recepción del mismo por la entidad demandada, no constituye comunicación de su solicitud de acceso o cancelación, pues "serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas, del contenido íntegro de las comunicaciones y se identifique fidedignamente al remitente y al destinatario de las mismas"[345]. De esta forma, la mera aseveración de la remisión de un mensaje privado a la red social no legitima para proceder a solicitar el procedimiento de tutela de derecho.

Respecto a la naturaleza de las alegaciones realizadas por motivo de las reclamaciones de tutela de derechos, como mencionamos, residen en la denegación del ejercicio de su derecho de acceso o cancelación, o incumplimiento al deber de información por parte del responsable o encargado del fichero, radicando la generalidad de las alegaciones fundadas

[345] ESPAÑA. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (Vigente hasta el 02 de octubre de 2016). artículo 27.3.

en publicaciones sin su consentimiento de sus datos personales en las redes sociales.

El presente apartado se centrará en analizar el principal criterio desarrollado por la AEPD para fundamentar su legítima competencia para fiscalizar y sancionar a los proveedores de servicios de redes sociales, tales como Facebook y Twitter, en conformidad a la normativa española.

Tal criterio ha sido utilizado en todas las resoluciones que han sido analizadas de la AEPD, aun en aquellos casos en que ha debido desestimar las reclamaciones de tutela de derecho por incumplimiento a los requisitos del artículo 5 de la LOPD por parte de los reclamantes.

A continuación se analizará un caso en concreto[346], centrando dicho estudio en lo que respecta a fundamentar la subordinación de Facebook a la normativa española y, en consecuencia, la obligatoriedad de índole legal

[346] En este caso el interesado solicitaba a Facebook Spain S.L, la eliminación de sus datos personales que aparecían en una publicación en la que se realizan una serie de afirmaciones sobre el interesado, sin fundamento y que faltan a la verdad, asimismo se trata de una cuestión antigua, sin interés público y que ya ha sido aclarada por los tribunales españoles. En estos momentos el procedimiento judicial ya terminó, las recusaciones se sustancian ante los tribunales y además sobre el asunto, que llegó al Tribunal Supremo, recayó sentencia en la que, respecto a la recusación, se determinó que no había lugar a ella." Por tanto procedería eliminarse dicho contenido. ESPAÑA. AEPD. Resolución N° R/02681/2015.

que esta entidad tiene respecto a cumplir con la solicitud de derecho de cancelación del afectado, así como demás requerimientos por parte del a Agencia Española de Protección de Datos.

Lo anterior se debe a que la red social en todos los traslados que ha evacuado a la AEPD ha señalado que Facebook Spain S. L. no es ni responsable, ni encargada de los contenidos alojados en la web. Alegando que es Facebook Ireland Limited el proveedor del servicio de los usuarios de Facebook en España y de la Unión Europea, entidad que está constituida en conformidad a las leyes de Irlanda.

En consecuencia, la AEPD analiza dos elementos:

- ¿Es aplicable la normativa comunitaria de protección de datos personales tanto a Facebook Spain, Facebook Ireland y Facebook Inc.?
- En caso afirmativo, ¿cuál es la legislación nacional aplicable?

En primer lugar, el informe analiza si se dan las condiciones para considerar a Facebook como responsable de tratamientos de datos en los términos de la normativa comunitaria de la UE.

La respuesta de la AEPD es afirmativa, fundamentando su criterio en la interpretación del artículo 3 del RLOPD, el cual es la transposición al artículo 4 de la Directiva 95/46/CE. Este señala, en síntesis, que estas disposiciones se aplican al tratamiento de datos personales efectuado por las redes sociales en varios casos, incluso cuando sus oficinas centrales se encuentran situadas fuera de los estados del espacio económico europeo.

Refuerza este postulado, al citar el Dictamen 5/2009 sobre redes sociales en línea, arguyendo que este documento se centra en cómo el funcionamiento de los servicios de las redes sociales (SRS) puede satisfacer los requisitos de la legislación sobre protección de datos de la Unión Europea. Señala que los proveedores de redes sociales[347] son responsables del tratamiento de datos en los términos estipulados en la Directiva 95/46/CE, pues no procede aplicar la exención de carácter doméstico.

En conclusión, la AEPD señala que los proveedores de SRS son responsables del tratamiento de dato en virtud a la directiva relativa a la protección de datos, unido a la no aplicación de la exención de carácter domestico de la situación objeto de la reclamación, determinan que

[347] ESPAÑA. AEPD. Procedimiento de tutela de derechos. N° TD 878/2015.

Facebook es responsable del tratamiento acaecido en el presente caso de conformidad a la normativa comunitaria.

En segundo lugar, la AEPD analiza la procedencia de la aplicación de la legislación española, pues el Dictamen 5/2009 del GT29 no analiza la ley nacional aplicable, sino que remite el análisis de ello al Dictamen 1/2008 relativo a los motores de búsqueda.

De este modo, el Dictamen 1/2008 viene en adecuar la interpretación del artículo 4° de la Directiva 95/46/CE en el ámbito de los motores de búsqueda, lo que en opinión del GT29 se aplica de forma análoga a las redes sociales, en virtud de la naturaleza transnacional de los flujos de datos. Así, se pretende evitar vacíos en el sistema establecido para la protección de datos en la Comunidad Europea y, además, evitar la posibilidad de que la misma operación de tratamiento se rija por leyes de más de un Estado miembro de la UE.

Así, en los términos del artículo 4° (a) de la Directiva 95/46/CE se considera que Facebook tiene un establecimiento en territorio español, ya que se acredita el ejercicio real y efectivo de actividades dentro de esta zona

geográfica. Fundamentándose en el siguiente criterio construido por el GT29:

> "Cuando el proveedor establece una oficina en un Estado miembro, implicada en la venta de anuncios dirigidos a los habitantes de dicho estado"[348].

La AEPD aplica dicho criterio, señalando en el caso concreto que Facebook Inc. presta un servicio remunerado de publicidad, mediante la venta del espacio publicitario. Para esta actividad se sirve de promotores locales, como Facebook Spain S. L., que incentiva la compra de espacio en el área que tiene atribuida[349].

En consecuencia, en virtud del artículo 4.a de la Directiva 95/46/CE se acredita que la legislación aplicable contra Facebook Inc., y su filial Facebook Spain S. L., es la legislación de España, contenida en la LOPD. Luego, la AEPD señala que en virtud del artículo 4.c de la Directiva 95/46/CE también procede aplicar la legislación española. De esta forma, en

[348] Grupo de Trabajo sobre Protección de Datos del Artículo 29. Dictamen de 4 de abril de 2008 sobre cuestiones de protección de datos en relación con buscadores. [en línea] <https://www.agpd.es/portalwebAGPD/canaldocumentacion/internacional/common/pdf/WP_148_DictamenBuscadores_es.pdf>[consulta: 29 de noviembre de 2015]
[349] Ibíd. 12p.

todos aquellos casos en que el responsable del tratamiento no esté establecido en el territorio de la comunidad y recurra, para el tratamiento de datos personales, a *medios* situados en territorio español, procede aplicar la LOPD.

En efecto, el GT29 ha entendido que "la utilización de *cookies* y dispositivos de software similares por parte de un proveedor de servicios online también puede considerarse como recurso a medios en el territorio del Estado miembro, invocando, de este modo, la legislación en materia de protección de datos de dicho Estado miembro", lo cual es perfectamente aplicable en el caso de Facebook, y demás redes sociales, pues es sabido que utilizan *cookies* y diversas aplicaciones para rastrear y tratar los datos de sus usuarios.

Sin quedar conforme con dicha fundamentación, la AEPD termina su análisis señalando "no es solo la normativa específica de protección de datos la que, con arreglo a los argumentos anteriores, determina la Ley nacional aplicable a este supuesto, sino que dicha normativa resultaría en todo caso aplicable por determinación del tenor literal de la Ley 34/2002 de

Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)"[350].

Del análisis anterior, queda acreditado que el director de la Agencia Española de Protección de Datos actúa como órgano competente para velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, atendiendo a la reclamación formulada por los reclamantes, puede requerir a los servicios de redes sociales la adopción de medidas necesarias para la adecuación a las disposiciones de la LOPD, ejerciendo en consecuencia las funciones que le atribuye su artículo 37, así como los efectos establecidos en los artículos 8 y 17 de la LSSI.

En consecuencia, si bien en todos los casos Facebook y Twitter accedían al requerimiento de la Agencia cumpliendo con lo solicitado por el interesado, estas entidades argumentaban que lo hacían debido a que consideraron que en ciertos casos se incumplían las condiciones y políticas de la red social por parte del usuario denunciado, y, en otros, señalaban que accedían sin mayor fundamentación. Sin embargo, como bien quedó

[350] Ibíd. 13p.

acreditado por la Agencia, el cumplimiento de los requerimientos tiene su fundamento en la legislación española, y no en un mero acto de buena fe.

2.2. Resoluciones sancionadoras.

A diferencia del procedimiento de tutela de derechos, el cual se inicia siempre a instancia del afectado, el procedimiento sancionador en materia de protección de datos constituye una de las manifestaciones del *ius puniendi* del Estado, iniciándose siempre de oficio por el director de la AEPD, de conformidad a lo previsto en el artículo 122.2 del RLOPD[351]. No obstante, deba investigar de forma previa todas las denuncias que recibe. En consecuencia, es de competencia exclusiva de la AEPD valorar si existen responsabilidades de índole administrativas y decidir si se debe iniciar o no el procedimiento sancionador[352].

De las resoluciones sancionadoras que hemos analizado entre los años 2010 al 2015 que involucran el uso de las redes sociales, hemos de señalar que dichos procedimientos han sido iniciados por vulneración al artículo 6°

[351] Agencia Española de Protección de Datos. Procedimiento tutela de derechos. N° TD 330/2011. [en línea] <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2011/common/pdfs/TD-00330-2011_Resolucion-de-fecha-29-07-2011_Art-ii-culo-16-LOPD.pdf>[consulta: 29 de noviembre de 2015] 4p.
[352] ESPAÑA. RLOPD. artículo 11.2.

de la LOPD, es decir, por tratar datos de carácter personal sin que conste el consentimiento inequívoco del afectado, lo cual configura una infracción grave en virtud de lo establecido en el artículo 44.3 letra C de la LOPD, asociada al pago de una multa desde 60.000 euros hasta 300.000 euros.

Si bien se puede pensar que en la mayoría de estos casos simplemente bastaba con ejercer el derecho de cancelación instando al responsable o encargado del fichero solo a eliminar la información en cuestión, la AEPD ha considerado que en ciertos casos es pertinente el inicio del procedimiento sancionador, en consecuencia imponer multas, en virtud del siguiente criterio:

> "La naturaleza de los datos y la gravedad de los derechos hacen necesarios utilizar el procedimiento sancionador para sancionar una conducta no amparable en las reglas de internet sin que quepa limitarse a exigir la cancelación"[353].

De esta forma, se desprende de las diversas resoluciones analizadas que, si son datos considerados especialmente protegidos, tales como: publicaciones de licencias médicas, preferencias religiosas, tendencias

[353] ESPAÑA. AEPD. Procedimiento Sancionador. N° PS 174/2012 y N° PS 595/2012.

políticas, entre otras; y, la gravedad de los derechos, tales como: la creación de perfiles falsos o la divulgación de información personal con la intención de perjudicar a su titular, así como la transgresión al deber de secreto profesional[354], en estos casos la AEPD iniciará el procedimiento sancionador al ser considerada una conducta especialmente grave no amparable en las reglas de internet[355].

2.2.1. Principales criterios considerados por la Agencia para la resolución de los conflictos en el ámbito de las redes sociales.

La Agencia, para desarrollar su criterio conforme a derecho, debe esclarecer una serie de interrogantes respecto a la aplicabilidad de la LOPD y demás normativa comunitaria en el caso en concreto. De esta forma, la AEPD considera una serie de elementos en su análisis, tales como: la naturaleza jurídica de los datos denunciados; el consentimiento inequívoco

[354] La recurrente, como garante de los datos personales de terceros que figuraban en sus ficheros, no tuvo la diligencia exigible sino que propició la revelación como cooperador necesario por omisión. Siendo ello así, la Sala entiende cometida, como también recoge la resolución impugnada, la infracción del artículo 10 de la LOPD, tipificada en el artículo 44.3.g de la citada norma, es decir la vulneración del deber de guardar secreto. ESPAÑA. AEPD. Procedimiento Sancionador. N° PS 165/2015.

[355] Agencia Española de Protección de Datos. Procedimiento Sanacionador. N° PS 764/2010. [en línea] <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2011/common/pdfs/PS-00764-2010_Resolucion-de-fecha-29-04-2011_Art-ii-culo-6.1-LOPD.pdf> [consulta: 29 de noviembre de 2015] 5p.

del afectado; procedencia de la exención doméstica e identificación del responsable del tratamiento de datos.

A continuación, se procederá a describir cada uno de estos elementos, a través de las diversas resoluciones emanadas de la AEPD que han sido analizadas por motivo del procedimiento sancionador.

i) Naturaleza jurídica de los datos denunciados.

En primer lugar, la AEPD debe establecer si el contenido denunciado es considerado un dato personal en los términos del artículo 3° de la LOPD. Esto es, cualquier información concerniente a personas físicas identificadas o identificables, siendo complementada esta definición por el artículo 5° del RLOPD al definir, como dato personal, "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables".

Luego, procede a analizar si dicho dato personal es de aquellos especialmente protegidos de acuerdo a lo estipulado en el artículo 7 del mismo cuerpo legal, es decir, aquellos datos que revelen la ideología, afiliación sindical, religión y creencias.

La AEPD ha considerado que "la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones constituye un 'tratamiento total o parcialmente automatizado de datos personales' en el sentido del artículo 3, apartado 1, de la Directiva 95/46"[356]. En consecuencia, la divulgación de dichos datos de carácter personal debe cumplir con la normativa contenida en la LOPD.

En el ámbito de las redes sociales, diversos son los casos en los cuales se difunden este tipo de información, sin embargo, de acuerdo a las resoluciones que hemos analizado, la mayoría tiene por finalidad denostar al titular de dichos datos. A modo de ejemplo, se puede destacar el caso en el cual la denunciante alega la difusión sin su consentimiento, de su apodo y primer apellido, dirección y horario laboral, así como de una fotografía en

[356] Agencia Española de Protección de Datos. Procedimiento Sancionador. N° PS 620/2014. [en línea] <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2015/common/pdfs/PS-00620-2014_Resolucion-de-fecha-28-04-2015_Art-ii-culo-6.1-LOPD.pdf>[consulta: 29 de noviembre de 2015]

la red social Facebook, con la intención de difundir el rumor de que esta tiene sida, todo por motivo de una venganza sentimental[357].

En la resolución de este caso, la AEPD consideró que, ciertamente, el contenido de los datos difundidos era de índole personal, sumado a que no se requirió el consentimiento inequívoco de su titular y sin que concurriera alguna de las excepciones contenida en el artículo 2 de la LOPD. La Agencia ordenó a Facebook Inc. la eliminación de dicho contenido e impuso una multa a pagar de 2.000 euros a la persona responsable de la difusión de dicho contenido. Por regla general, la difusión de este tipo de datos que no son especialmente protegidos no acarrea responsabilidad, no obstante, la AEPD considera que, de forma excepcional, pueden tener naturaleza de datos protegidos, dependiendo de cada situación en particular.

Así, es importante de destacar el caso en el cual una denunciante alega que se ha extraído su nombre completo, desde un grupo privado de Facebook, con la finalidad de incluirlo en una lista publicada en un blog,

[357] Agencia Española de Protección de Datos. Procedimiento Sancionador. N° PS 595/2012. [en línea] <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2013/common/pdfs/PS-00595-2012_Resolucion-de-fecha-11-02-2013_Art-ii-culo-6-LOPD_Recurrida.pdf>[consulta: 29 de noviembre de 2015]

asociándola como miembro de la comunidad Opus Dei, sin que dicho blog obtuviera su consentimiento expreso ni respetara su derecho de cancelación exigido en forma previa[358].

La AEPD estimó de tal gravedad el tratamiento de los datos especialmente protegidos "que no puede ser tomada en consideración la solicitud del denunciado de que se tenga en cuenta que no tiene precedentes sancionadores o de apercibimiento, debiendo atenderse a la naturaleza de los datos publicados de la denunciante y de, al menos, otras 158 personas, a las que también se incluyó en un listado públicamente accesible y se atribuyó unilateralmente la pertenencia a una determinada organización religiosa, negándoseles la posibilidad de cancelación a menos que públicamente declararan su no vinculación con la misma"[359]. Por lo que el denunciado fue condenado a eliminar el listado de su blog y a pagar una multa de 2.000 euros, sin ser beneficiado con la graduación de la culpa.

[358] Agencia Española de Protección de Datos. Procedimiento Sancionador. N° PS 337/2011. [en línea] <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2012/common/pdfs/PS-00337-2011_Resolucion-de-fecha-11-01-2012_Art-ii-culo-6.1-LOPD.pdf >[consulta: 29 de noviembre de 2015]

[359] Ibíd.13p.

En el caso de las fotografías y videos compartidos en las redes sociales, la AEPD estima que se considerarán datos personales en la medida que permitan la identificación de las personas que aparecen en dichas imágenes. Podrán estos llegar a ser considerados como dato sensible en la medida que estos se utilicen para revelar datos sensibles de los individuos[360]. Esto, porque la Agencia sigue el criterio del GT29 al considerar que, por regla general, las imágenes en internet no son datos sensibles[361].

Asimismo, la AEPD señala que aun las imágenes de las personas captadas en lugares públicos constituyen un tratamiento de datos personales incluido en el ámbito de aplicación de la normativa citada[362], lo cual estimo que tiene directa relación con la expectativa de privacidad que poseen las personas incluso en lugares públicos; por tanto, es improcedente que se difundan dichas imágenes y, más aun, cuando dicha difusión tiene por finalidad denostar a las personas que figuran en ellas.

La AEPD ha recibido varias denuncias de esta índole. Destaca el caso en el cual el autor de un montaje de video es denunciado por utilizar en dicha

[360] Agencia Española de Protección de Datos. Procedimiento Sancionador. N° PS 446/2011. 11p.
[361] Agencia Española de Protección de Datos. Procedimiento N° PS 174/2012. p.6.
[362] Agencia Española de Protección de Datos. Procedimiento N°: PS 764/2010. p. 3.

grabación fotografías de una pareja obtenidas de diversos viajes y fiestas compartidas, sin su consentimiento, y además con la intención de burlarse de ellos, difundiendo el contenido de dicho video por la red social Facebook, pudiendo tener acceso cualquier persona a él[363].

También destaca el caso donde un par de hermanas ven difundidas fotografías de ellas, incluyendo aquellas de carácter íntimo, en Facebook con la intención de difamarlas, insultarlas y amenazarlas, todo como consecuencia de una venganza por una ruptura sentimental[364].

En estos casos, la AEPD ha considerado que dichas acciones son un elemento a considerar para iniciar el procedimiento sancionador y no requerir simplemente la cancelación de los datos, pues ciertamente queda en evidencia la gravedad de la transgresión de estos derechos y, en consecuencia, procede la imposición de una multa.

Es importante hacer mención a la naturaleza jurídica del correo electrónico, puesto que, en el ámbito de las redes sociales, equivale a nuestra cédula de identidad digital, por cuanto estos servicios exigen la

[363] Ibíd.
[364] Agencia Española de Protección de Datos. Procedimiento Sancionador. N° PS 721/2014.

indexación de un e-mail para poder hacer uso de estos servicios e identificarnos a nivel operacional.

La AEPD ha señalado que no todo correo electrónico tiene la naturaleza de dato personal, salvo que se configure el siguiente supuesto:

> "La dirección de correo electrónico de una persona física, en la medida que permite identificar a su titular sin plazos ni actividades desproporcionadas, constituye un dato personal y su tratamiento en casos como el presente, y sin perjuicio de las previsiones específicas establecidas por la Ley de Servicios de Sociedad de la Información para otros supuestos, está sometido a las previsiones de la LOPD"[365].

De esta forma, la AEPD multó a una organización a pagar 3.000 euros por no requerir el consentimiento inequívoco de la denunciante respecto a poder enviarle información a su e-mail, el cual estaba conformado por el

[365] Agencia Española de Protección de Datos. Procedimiento Sancionador. N° PS 449/2012. [en línea] <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2013/common/pdfs/PS-00449-2012_Resolucion-de-fecha-07-03-2013_Art-ii-culo-6.1-LOPD.pdf> [consulta: 29 de noviembre de 2015] 7p.

nombre y apellido de su titular, el cual fue obtenido por uno de sus contactos de Facebook desde su perfil[366].

ii) El consentimiento inequívoco del afectado y la exención doméstica.

La Agencia, luego de confirmar que se está en presencia de un contenido que tiene la naturaleza de dato personal, analizará si a dicho dato personal le es aplicable el régimen jurídico contenido en la LOPD. Ya que el artículo 2 del referido cuerpo legal, entre las excepciones que señala, establece que no se aplicará la LOPD en aquellos "ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas".

La AEPD para desarrollar dicho análisis, considera el Dictamen 5/2009 del GT29, descrito en el capítulo anterior, estimando en todos estos casos que el tratamiento de los datos personales de los afectados por parte de los denunciados excede el ámbito privado o doméstico, pues hemos de recordar que la mayoría de los casos analizados tenían por finalidad denostar al titular de dicha información u obtener algún beneficio de índole económico por la recolección de dichos datos a través de las redes sociales[367].

[366] Ibíd.
[367] Agencia Española de Protección de Datos. Procedimiento Sancionador. N° PS 210/2014. [en línea]

La AEPD, luego de establecer que se ha tratado un dato de carácter personal o especialmente protegido y que no concurre alguna de las excepciones contenidas en el artículo 2 de la LOPD, debe analizar si dichos datos se obtuvieron de fuentes de acceso público. Sin embargo, la Agencia ha señalado que el tratamiento de los datos de carácter personal que figuran en internet (en el presente caso, la fotografía de la denunciante recabada de la red social Facebook) por persona o entidad distinta a los interesados precisa el consentimiento previo de los mismos, no pudiendo considerarse que tal fuente es de acceso público"[368].

Lo anterior radica en que el artículo 3.j de la LOPD es taxativo, y no señala dentro de esta clasificación a las páginas web, menos aún las redes sociales. Por ello, en el ámbito de las redes sociales será necesario recabar el consentimiento inequívoco del titular de dichos datos en conformidad a la LOPD.

<http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2014/common/pdfs/PS-00210-2014_Resolucion-de-fecha-23-09-2014_Art-ii-culo-6.1-LOPD.pdf> [consulta: 29 de noviembre de 2015]

[368] Agencia Española de Protección de Datos. Procedimiento Sancionador. N° PS 446/2011.[en línea] <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2012/common/pdfs/PS-00446-2011_Resolucion-de-fecha-29-02-2012_Art-ii-culo-6-LOPD.pdf> 7p.

La Agencia señala que la LOPD no requiere que el consentimiento se preste por escrito o con formalidades determinadas, pero sí exige que este sea inequívoco en virtud de lo establecido en el artículo 6 de la LOPD. Entendiéndose lo anterior como aquella manifestación de voluntad que "no admite duda o equivocación y, por contraposición, a equívoco, lo que no puede entenderse o interpretarse en varios sentidos, o que no puede dar ocasión a juicios diversos"[369]. Sin embargo, la Agencia señala que ante la realidad de internet, no es conveniente realizar una interpretación maximalista del requerimiento de consentimiento, por tanto, se debe adecuar la normativa en cada caso concreto.

Así, la Agencia Española de Protección de Datos, en un caso en que el denunciado alegó que obtuvo el consentimiento de los denunciantes para publicar sus fotografías en una página comercial de Facebook, le solicitó "que para que dichas manifestaciones puedan ser tenidas en cuenta a efectos probatorios, es necesario que nos remita Acta de Manifestaciones realizadas ante Notario o mediante cualquier otro documento válido en Derecho que

[369] Agencia Española de Protección de Datos. Procedimiento Sancionador. N° PS 434/2011. [en línea] <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2012/common/pdfs/PS-00434-2011_Resolucion-de-fecha-16-02-2012_Art-ii-culo-6.1-LOPD.pdf> [consulta: 29 de noviembre de 2015] 8p.

acredite fehacientemente la identidad de las personas que suscriben las manifestaciones de que se trata. Remitiendo el Acta de Manifestaciones o el citado documento, a esta Agencia en el plazo de diez días hábiles a la recepción del presente escrito"[370]. Lo cual efectivamente fue cumplido por el denunciado, y en consecuencia fue exonerado de todos los cargos por parte de la AEPD.

Ahora, respecto al tratamiento de los datos especialmente protegidos, la AEPD ha señalado por motivo de la publicación en Facebook de una licencia médica, sin el consentimiento expreso del denunciante, que "los datos personales sensibles solo se pueden publicar en internet con el consentimiento explícito del sujeto de datos o si el sujeto de datos ha hecho que los datos sean manifiestamente públicos él mismo"[371]. Lo cual no se configuró en el presente caso, pues la licencia fue difundida a través de la página de Facebook de la empresa para la cual trabajaba el denunciante.

---

[370] Agencia Española de Protección de Datos. Procedimiento Sancionador. N° PS 2/2010. [en línea] <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2010/common/pdfs/PS-00002-2010_Resolucion-de-fecha-07-06-2010_Art-ii-culo-6.1-LOPD.pdf> [consulta: 29 de noviembre de 2015] 3p.

[371] Agencia Española de Protección de Datos. Procedimiento Sancionador. N° PS 434/2011. [en línea] <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2012/common/pdfs/PS-00434-2011_Resolucion-de-fecha-16-02-2012_Art-ii-culo-6.1-LOPD.pdf>[consulta: 29 de noviembre de 2015] p. 8.

iii) Identificación del responsable del tratamiento de datos.

En primer lugar, se debe aclarar que para la AEPD las páginas web y, en consecuencia, el perfil de una red social, cumplen con los requisitos de ser considerados ficheros. Estos permiten "cualquiera sea su finalidad una organización o estructura que permite el acceso a la información en el contenida por terceros". Y luego señala: "Si hubo tratamiento de datos de carácter personal consistente en la incorporación y difusión de estos desde una estructura organizada (fichero) como era el sitio web, es indudable que el régimen de protección contenido en la Ley Orgánica 15/1999 es plenamente aplicable"[372].

En consecuencia de lo anterior, una página o perfil de Facebook puede ser considerado un fichero en los términos de la LOPD y, en consecuencia, el usuario titular de dicha página o perfil es responsable del tratamiento de datos.

[372] Agencia Española de Protección de Datos. Procedimiento Sancionador. N° PS 337/2011. [en línea] <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2012/common/pdfs/PS-00337-2011_Resolucion-de-fecha-11-01-2012_Art-ii-culo-6.1-LOPD.pdf> [consulta: 29 de noviembre de 2015] 9p.

Existen ciertos casos en que ha sido complejo para la AEPD identificar al responsable del tratamiento indebido de datos en las redes sociales. La solución que ha implementado la Agencia es requerir información de la IP a las redes sociales y al servicio de telecomunicaciones local.

Lo anterior se debe a que la AEPD ha adoptado el criterio de la sentencia de 20/10/2011, en la cual la Audiencia Nacional confirmaba la sanción impuesta por la Agencia al titular de una línea telefónica desde la que se había colgado un video en internet. En esta sentencia se argumentaba: "En este caso, quien incluye el video en YouTube es el responsable del tratamiento pues decide, a través de dicha inclusión en internet, sobre la publicación y difusión del citado video, y en definitiva sobre la finalidad del tratamiento, ostentando la condición de responsable del tratamiento. Puesto que, como se ha expuesto anteriormente de forma detallada, el video fue incluido en la cuenta de usuario utilizando la 'contraseña' de YouTube y la cuenta y contraseña fueron creadas desde la línea titularidad del recurrente instalada en su domicilio, debe considerarse al recurrente responsable del tratamiento y, por tanto, responsable de la infracción por el tratamiento

inconsentido de datos consecuencia de la inclusión del video en YouTube"[373].

Mismo criterio se utilizó en el caso que anteriormente comentamos, respecto a la difusión de una licencia médica en la página de Facebook de la empresa donde trabajaba el denunciante, pues dicha empresa alegó que no tenía responsabilidad en el asunto y que, además, era complejo saber la identidad de la persona que divulgó dicho contenido, pues una gran cantidad de trabajadores tenían acceso al usuario y contraseña de dicha página.

Sin embargo, la AEPD condenó de todos modos a la empresa, pues comprobó que las conexiones a dicho perfil se realizaron utilizando las líneas telefónicas de ella, además de ser esta la titular de dicho perfil. Por ello, la carga de la prueba se trasladó a la empresa en virtud de la normativa civil[374], la empresa debía probar que obtuvo el consentimiento expreso para

[373] Agencia Española de Protección de Datos. Procedimiento Sancionador. N° PS 174/2012. [en línea] <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2012/common/pdfs/PS-00174-2012_Resolucion-de-fecha-20-07-2012_Art-ii-culo-6.1-LOPD.pdf> [consulta: 29 de noviembre de 2015] 7p.
[374] ESPAÑA. Código Civil. artículo 1.214.

difundir la licencia médica en su página de Facebook, situación que no acaeció.

Para finalizar, es importante mencionar que la AEPD ha señalado que para proceder a analizar la gradación de la culpa en los términos del artículo 45.4 se considera el volumen de los datos personales accedidos, la ausencia de reincidencia en la comisión de infracciones de la misma naturaleza y el volumen de negocio o actividad de la imputada[375], no accediendo la AEPD a utilizar la graduación de la culpa en aquellos casos en que se trataron datos especialmente protegidos de más de cien personas obtenidos desde la red social Facebook.

2.2.2. Conflicto del bien jurídico protegido.

La AEPD en algunas oportunidades ha tenido que hacer referencia al conflicto de bienes jurídicos protegidos que se origina con el uso de las redes sociales, por tanto ha debido determinar si prevalece el derecho a la protección de datos personales o el derecho a la información, basado en la satisfacción del interés general.

[375] Agencia Española de Protección de Datos. Procedimiento Sancionador. N° PS 449/2012.

Así, acontinuación se procederá a esclarecer el criterio construido por la AEPD, analizando el caso PS/00449/2012[376]. La denunciante en este procedimiento ha declarado que viene recibiendo envíos masivos de correos electrónicos sin su autorización por parte de los administradores de una corporación, quienes obtuvieron su e-mail desde el perfil de Facebook de la denunciante.

La AEPD procedió a dar traslado a la entidad denunciada, la cual manifestó que: "Se han limitado a transmitir una información veraz, de interés general, y en el ejercicio de su derecho constitucional a la libertad de información, actuando adecuadamente por la necesidad de satisfacer un interés legítimo y por el compromiso ante los ciudadanos en su labor de participación política".

En consecuencia, la AEPD se vio obligada a esclarecer qué derecho prevalece en el presente caso, es decir, si prevalece el derecho a la protección de datos personales de la denunciante y, en consecuencia, procede sancionar a la corporación, o si por el contrario debe exonerar de

[376] Ibíd.

los cargos a dicha entidad en resguardo de su derecho a la libertad de información.

La AEPD cita la jurisprudencia del Tribunal Constitucional señalando que para que prevalezca el derecho a la libertad de información, los hechos comunicados deben ser considerados de relevancia pública y además se debe atender a la veracidad de la información facilitada[377].

La AEPD señala que en el presente caso no se dan estos elementos y, en consecuencia, prevalece el derecho a la protección de datos personales, sin perjuicio de que "en determinados supuestos es posible que la ponderación pudiera operar a favor de los principios puestos de manifiesto en las alegaciones, como podría suceder en el caso de que la comunicación se hubiera remitido en el período de campaña electoral, tal circunstancia no se da en el presente caso, lo que conduce necesariamente a la desestimación de las alegaciones" realizadas por la corporación. Pues, en efecto, en opinión de la AEPD, al no ser periodo de elecciones dicha comunicación pierde relevancia pública.

[377] Ibíd. 9p.

En consecuencia, al constatar que la corporación no requirió el consentimiento de la denunciante para poder tratar sus datos, la AEPD condenó a dicha entidad una multa de 3.000 euros.

De lo anterior, es posible verificar el ejercicio de las tres potestades de mayor trascendencia de la AEPD en el ámbito de las redes sociales.

Así, la potestad preventiva se observa en las diversas recomendaciones y requerimientos que realiza la Agencia a las redes sociales; para que estas adecúen sus condiciones de uso y política de privacidad, al estándar adecuado exigido a nivel comunitario; así como también consta que el ciudadano español cada día es más consciente de los derechos que tiene en el ámbito de internet, y en consecuencia en las redes sociales.

La potestad de inspección o fiscalización de la Agencia se desprende tanto de los diversos requerimientos que realiza la AEPD en la investigación de los sucesos como del procedimiento de tutela de derechos y del procedimiento sancionador. Mientras que la potestad sancionatoria, por su parte, se observa en el momento en que la AEPD condena al pago de una multa a aquellos usuarios y proveedores de servicios que han infringido la LOPD.

Cabe destacar que la Agencia a través de los diversos informes, documentos, resoluciones, entre otros, ciertamente ha conseguido mantener la vigencia de la normativa imperante de privacidad y datos personales, mediante la construcción de sus fundamentos en base a los principales lineamientos comunitarios y normativa interna, pues en las diversas consideraciones que hemos estudiado en el presente capítulo queda comprobado la subordinación de las redes sociales a la normativa española, por lo que no procede que estas excusen su cumplimiento por un simple acto de buena fe.

Asimismo, consta la intención de la AEPD por no afectar mediante la dictación de sus resoluciones el derecho a la información. De esta forma, siempre considerará en sus decisiones la relevancia de la información y la veracidad de los hechos, pues la protección de los datos en el ámbito de las redes sociales no debe ser una excusa para censurar la información en la red.

CONCLUSIONES.

El derecho a la vida privada ha mutado a lo largo del tiempo tanto a nivel doctrinal como jurisprudencia. Si bien en sus inicios era considerado una emanación del derecho de propiedad, posteriormente con el desarrollo de los derechos humanos, y en específico el valor de la dignidad, se consagró a nivel fundamental como un derecho autónomo desde una perspectiva negativa, manifestada en el derecho a ser dejado solo.

Con el transcurso del tiempo y ante el progreso de las tecnologías de la información y comunicación, nuevas amenazas surgieron contra la privacidad de las personas, siendo necesario volver a redefinir el contenido y alcance de este derecho por parte de la doctrina y jurisprudencia. Como consecuencia de lo anterior, surgió la necesidad de proteger la perspectiva positiva e informacional de este derecho, manifestado en el derecho a la protección de datos personales, el cual se concreta en la facultad de control que tiene el titular de los datos personales respecto al tratamiento de estos.

En Chile, si bien el derecho a la vida privada está consagrado a nivel constitucional, los intentos de sistematización de la jurisprudencia existente

en temas de privacidad han sido precario por parte de la doctrina y judicatura. Lo anterior se debe, por una parte, a la dificultad de determinar el bien jurídico protegido en el ejercicio de la acción de protección, y, por otra, a la ineficacia de la acción *habeas data* ejercida únicamente en sede judicial.

Sumado a lo anterior, desde la perspectiva específica del derecho a la protección de datos personales, se han detectado una serie de falencias en la actual normativa contenida en la Ley 19.628, destacando entre ellas la ausencia de una autoridad de control que se encargue de fiscalizar el cumplimiento de esta ley, sanciones con bajas multas asociadas, la inexistencia de una obligación de registro de datos de índole privado, inexistencia de potestades de oficio para poder inspeccionar y fiscalizar en cumplimiento de la ley, entre otras. En consecuencia, la comunidad internacional ha llegado a considerar a Chile como un país que no cumple con un estándar adecuado de privacidad.

Al contrario de nuestra realidad nacional, la labor interpretativa de la judicatura española es destacable, pues ha desarrollado el concepto de intimidad y protección de datos de carácter personal a lo largo del tiempo,

logrando adaptar su contenido al tiempo y cultura actual. Lo anterior se debe a la vasta normativa promulgada sobre este tema, lo que sumado a la legislación imperante a nivel comunitario ha permitido a España adecuar la interpretación de sus normas frente a las nuevas amenazas que se generan en el ámbito de internet y, en específico, con el uso indebido de las redes sociales.

La labor de la Agencia Española de Protección de Datos ha sido trascendental para asegurar el cumplimiento de la normativa de privacidad y datos personales en la época actual. Esto se debe a que el mismo constituyente le ha reconocido independencia funcional y una serie de potestades, destacando entre ellas las de prevención, fiscalización y sanción, las cuales son ejercidas de forma efectiva en el ámbito de las redes sociales.

Ante la nueva realidad de estas plataformas y lo complejo de aplicar la normativa vigente en este escenario que está en constante transformación, la UE, y en específico España, han desarrollado diversos criterios con el afán de evitar la desprotección e incumplimiento del derecho a la privacidad de los datos, pues las amenazas que surgen en este tipo de plataformas sociales

son innumerables, destacando la suplantación de identidad, el *pishing* y el tratamiento indebido de los datos con fines comerciales, entre otros.

Debido a estos riesgos, España con la finalidad de enfrentar este tipo de transgresiones ha desarrollado su criterio normativo en el ámbito de las redes sociales, considerando una serie de elementos, tales como el estándar Bodil Lindqvist, las principales recomendaciones del GT29 y las diversas resoluciones emanadas por parte de su Agencia de Protección de Datos. Todo lo anterior ciertamente ha reflejado resultados satisfactorios en la protección y cumplimiento del derecho a la protección de datos personales en el uso de estas plataformas virtuales.

Ahora, centrándonos en el caso de Chile, ante la disparidad de la normativa a nivel continental y el precario desarrollo de la legislación en el ámbito de internet, ha sido complejo adecuar la interpretación de la actual normativa en este aspecto. Además, es menester señalar que dicha complejidad se ha acrecentado debido a la ausencia de una autoridad de control independiente y especializada que otorgue eficiencia y eficacia a la legislación nacional.

De lo anterior se colige la imperiosa necesidad por parte de nuestro país de implementar diversas reformas a nivel legislativo con el afán de proteger la privacidad de los datos en el ámbito de internet, de las redes sociales y de futuras amenazas que surjan en el ámbito de la tecnología. Para tales efectos, consideramos ineludible el reconocimiento a nivel constitucional del derecho a la protección de datos personales, así como la pronta promulgación de la reforma de la Ley 19.628, y la consagración efectiva de una autoridad de control que asegure el cumplimiento de la ley.

Si bien estimo que la alternativa más razonable es la creación de una Agencia de Protección de Datos adecuada a nuestra realidad nacional, ciertamente es posible vislumbrar que no es una opción pronta a considerar ni por parte del gobierno ni el Congreso Nacional, por tanto, esperamos que en la actual reforma en tramitación se le otorguen verdaderas potestades de oficio, inspección y coerción tanto al SERNAC como al CPLT.

Finalmente, como prevención general, considero que la mejor forma de proteger los datos personales de los ciudadanos en el ámbito de las redes sociales es educando a la población respecto a los derechos que estos tienen, y dando a conocer los diversos peligros que conlleva la

sobreexposición de su privacidad en el ámbito de internet. Por tanto, la labor de prevención es trascendental en este sentido, con la finalidad de generar ciudadanos cautelosos y responsables en el resguardo de su privacidad, y así evitar además conflictos con otros derechos de igual trascendencia, como lo es el derecho a la libertad de opinión e información.

BIBLIOGRAFÍA.

LIBROS.

1. ARRIETA, Raúl. 2009. Chile y la protección de datos personales: compromisos internacionales. En: ¿Están en crisis nuestros derechos fundamentales? Serie de Políticas Públicas. Santiago, Ediciones Universidad Diego Portales.

2. ALMAIDA, C. A., COUDERT, F., PORTERA, A. M. & NAVALPOTRO, Y. N. 2007. Estudio práctico sobre la protección de datos de carácter personal. España, Editorial Lex Nova.

3. BADINTER, Robert. 1968. Le droit au respect de la vie privée. Francia, Editorial JPC G.

4. BLÁZQUEZ, Niceto. 2000. El desafío ético de la información. España, Editorial Edibesa.

5. CAMPUZANO, Herminia. 2000. Vida privada y datos personales: su protección jurídica frente a la sociedad de la información. España, Editorial Tecnos.

6. COOLEY, Thomas. 1906. A Treatise on the Law of Torts, Or the Wrong which Arise Independently of Contract. Callaghan, Chicago.

7. DELGADO, L. y SALTOR, C. 2014. El derecho a la protección de datos en España y Argentina: orígenes y regulación vigente. España, Editorial Dykinson.

8. DRUMMOND, Víctor. 2004. Internet, privacidad y datos personales. Madrid, Editorial Reus.

9. FIGUEROA, Rodolfo. 2015. Privacidad. Santiago, Editorial Universidad Diego Portales.

10. GÓMEZ, Gastón. 2005. Derechos fundamentales y recurso de protección. Santiago, Ediciones Universidad Diego Portales.

11. GONZÁLEZ, Jesús. 1986. La dignidad de la persona. Madrid, Editorial Civitas.

12.JIJENA, Renato. 1992. La protección penal de la intimidad y el delito informático. Santiago, Editorial Jurídica de Chile.

13.MADRID, Fulgencio. 1984. Derecho a la intimidad, informática y Estado de Derecho. Valencia, Universidad de Valencia.

14.NOVOA, Eduardo. 1979. Derecho a la vida privada y libertad de información. México, Siglo XXI Editores.

15.PEÑA, Carlos. 1996. El Derecho Civil en su relación con el Derecho Internacional de los Derechos Humanos. En: CILLERO, M. Sistema jurídico y derechos humanos: el derecho nacional y las obligaciones internacionales de Chile en materia de derechos humanos. Santiago, Universidad Diego Portales.

16.PÉREZ LUÑO, Antonio. 1984. Derechos humanos, Estado de Derecho y Constitución. Quinta Eduición. Madrid, Editorial Tecnos S.A.

17.PÉREZ LUÑO, Antonio. 2012. Los derechos humanos en la sociedad tecnológica. España, Editorial Universitas.

18.PFEFFER, Emilio. 1985. Manual de derecho constitucional, Tomo I. Santiago, Editorial Jurídica Ediar Conosur.

19. RODOTA, Stefano. 1973. Elaboratori elettronici e controllo sociale. Italia, Editorial Il Mulino.

20. VALLEJO, Antonio. 1994. Derecho a la intimidad e informática. España, Editorial Comares.

REVISTAS.

21. ALVARADO, Francisco. 2014. Las fuentes de acceso público a datos personales. Revista de derecho y tecnología. 3(2):205-226.

22. BANDA, Alfonso. 2000. Manejo de datos personales. Un límite al derecho a la vida privada. Revista de Derecho Valdivia 11: 55-70.

23. BELTRÁN, José. 2014. Aproximación al régimen jurídico de las redes sociales. Cuaderno Electrónico de Estudios 2: 61-90.

24. CALDEVILLA, David. 2010. Las redes sociales. Tipología, uso y consumo de las redes 2.0 en la sociedad digital actual. Documentación de las Ciencias de la Información (33):45-68.

25. CEA EGAÑA, José. 1996. El derecho constitucional a la intimidad. Revista Gaceta Jurídica (198):27.

26. CEA EGAÑA, José. 1993. Misión cautelar de la Justicia Constitucional. Revista Chilena de Derecho 20(2-3):395-408.

27. CERDA, Alberto. 2006. Mecanismos de control en la protección de datos en Europa. Ius et Praxis 12 (2):221-251.

28. CORRAL, Hernán. 2000. Configuración jurídica del derecho a la privacidad I: origen, desarrollo y fundamentos. Revista Chilena de Derecho 27(1): 53-54.

29. CORRAL, Hernán. 2001. La vida privada y la propia imagen como objetos de disposición negocial. Revista de Derecho, Universidad Católica del Norte, (8):159-175.

30. DOMÍNGUEZ, David. 2010. Las redes Sociales. Tipología, uso y consumo de las redes 2.0 en la sociedad digital actual. Documentación de las Ciencias de la Información (33):45-68.

31. FALCÓN, Javier. 1992. Los derechos del artículo 18 de la Constitución española en la jurisprudencia del Tribunal Constitucional. Revista Española de Derecho Constitucional 12(34).

32. FIGUEROA, Rodolfo. 2013. El derecho a la privacidad en la jurisdicción de protección. Revista chilena de derecho 40(3): 859-889.

33. GAZITÚA, M., SALINAS, C. y STANGE HANS, M. 2004. Intimidad y vida privada. Santiago, Centro de Estudios de la Comunicación Universidad de Chile.

34. GIL, Ana. 2012. El fenómeno de las redes sociales y los cambios en la vigencia de los Derechos Fundamentales. RDUNED. Revista de Derecho UNED **(**10):209-255.

35. JIJENA, Renato. 1999. Dominios, marcas y comercio electrónico en internet: anexo: la nueva ley chilena sobre la no protección de datos personales, Nº 19628 del 28 de agosto de 1999. Informática y Derecho: Revista Iberoamericana de Derecho Informático (30):365-418.

36. MARTÍNEZ, Ricard. 2007. El derecho fundamental a la protección de datos: perspectivas. IDP: Revista de Internet, Derecho y Política = Revista d'Internet, Dret i Política (5)47:61.

37. MARTÍNEZ, Eulalia. 2014. El procedimiento sancionador en la Agencia Española de Protección de Datos. Economist & Jurist 22(180):20-27.

38. MARTÍNEZ DE PISÓN, José. 1996. Vida privada e intimidad: implicaciones y perversiones. Anuario de Filosofía del Derecho (14):717-738.

39. MORALES, Fermín. 1984. Protección de la intimidad: delitos e infracciones administrativas. Cuadernos de Derecho Judicial (13):39-86.

40. MURILLO DE LA CUEVA, Pablo. 1999. La construcción del derecho a la autodeterminación informativa. Revista de Estudios Políticos (104):35-60.

41. MURILLO DE LA CUEVA, Pablo. 2008. El derecho a la autodeterminación informativa y la protección de datos personales. Azpilcueta: Cuadernos de Derecho (20): 43-58.

42. MURILLO DE LA CUEVA, Pablo. 1993. Informática y protección de datos personales: estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal. España, Centro de Estudios Constitucionales.

43.NOGUEIRA, Humberto. 2005. Autodeterminación informativa y habeas data en Chile e información comparativa. Anuario de Derecho Constitucional Latinoamericano 2(11):449-471.

44.NOGUEIRA, Humberto. 2007. El derecho a la propia imagen como derecho fundamental implícito: fundamentación y caracterización. Ius et Praxis 13 (2):245-285.

45.NOGUEIRA, Humberto. 2010. Dignidad de la persona, derechos fundamentales y bloque constitucional de derechos: una aproximación desde Chile y América Latina. Revista de Derecho (5):79-142.

46.PARDO, Javier. 1992. Los derechos del artículo 18 de la Constitución española en la jurisprudencia del Tribunal Constitucional. Revista Española de Derecho Constitucional 12(34).

47.PÉREZ LUÑO, Antonio. 1981. Informática y libertad. Comentario al artículo 18.4 de la Constitución Española. Revista de Estudios Políticos (24):31-53.

48.PIÑAR, José. 2003. La Agencia Española de Protección de Datos: estructura y funcionamiento. Revista Chilena de Derecho Informático (3):31-45.

49. PROSSER, William. Privacy (a legal analysis). Estados Unidos. California Law Review 48(383).

50. PUENTE, Agustín. 2008. La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal. Azpilcueta: Cuadernos de Derecho (20):13-41.

51. RALLO, A. y MARTÍNEZ, R. 2011. Protección de datos personales y redes sociales: obligaciones para los medios de comunicación. Quaderns del CAC 37 14(2):41-52.

52. RALLO, Artemis. 2009. La protección de datos en España: análisis de actualidad. Anuario de la Facultad de Derecho (2):15-30.

53. RAYMAN, Danny. 2015. Chile: vigilancia y derecho a la privacidad en internet. Revista Chilena de Derecho y Tecnología 4(1):187-232.

54. SOLOVE, Daniel. 2013. La autogestión de la privacidad y el dilema del consentimiento. Revista chilena de derecho y tecnología. 2(2):11-47.

55. SUÁREZ, Christian. 2000. El concepto de la vida privada en el derecho anglosajón y europeo. Revista Derecho de Valdivia (11):103-120.

56. TRONCOSO, Antonio. 2013. Las redes sociales a la luz de la propuesta del reglamento general de protección de datos personales: Parte dos. Revista d'Internet, Dret i Política (16):27-39.

57. VIAL, Tomás. 2000. Hacia la construcción de un concepto constitucional del derecho a la vida privada. Persona y Sociedad 14(3):47-68.

58. WARREN, Samuel. y BRANDEIS, Luis. 1980. The Right to Privacy. Harvard Law Review 4(5).

INFORMES Y ESTUDIOS.

59. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INTECO. 2009. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. [en línea] <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf> [consulta: 29 noviembre 2015].

60. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. 2010. Guía de Seguridad de Datos, [en línea] <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf> [consulta: 29 noviembre 2015].

61. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. 2014. Memoria 2014. [En línea] <http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2014/Memoria_AEPD_2014.pdf> [consulta: 29 noviembre 2015].

62. BAYTELMAN, Paloma. 2011. Protección de datos personales en la sociedad en redes. [en línea] <http://www.expansiva.cl/media/en_foco/documentos/18052011161648.pdf> [consulta: 29 noviembre 2015].

63. CONSEJO PARA LA TRANSPARENCIA. 2011. Recomendaciones sobre protección de datos personales por parte de los órganos de la Administración del Estado. [en línea] <http://www.cplt.cl/transparencia_activa/mecanismos/propuesta_de_rec

omendacion_pd_general_version_consulta_publica_11abril2011.pdf> [consulta: 29 noviembre 2015].

64. CHILE. 1980. Historia de la Ley Artículo 19 N° 4 de la Constitución Política de la República: El derecho a la privacidad. [en línea] <http://www.leychile.cl/Navegar/scripts/obtienearchivo?id=recursoslegales/10221.3/10540/1/HLArt19N_4.pdf>[consulta: 24 enero 2016].

65. CHILE. 1999. Historia de la Ley 19.628: Artículo 17 sobre protección de la vida privada. [en línea] <http://www.bcn.cl/obtienearchivo?id=recursoslegales/10221.3/2468/7/HL19628.pdf>[consulta: 24 enero 2016].

66. DERECHOS DIGITALES. Minuta de discusión: proyecto de ley que introduce modificaciones a la Ley N°19.628, sobre protección de la vida privada y protección de datos de carácter personal, 2012. [en línea] <https://www.derechosdigitales.org/wp-content/uploads/comentariosdd-datos.pdf> [consulta: 29 de noviembre de 2015]

67. JERVIS, Paula. 2006. La regulación del mercado de datos personales en Chile [en línea] <http://www.repositorio.uchile.cl/handle/2250/114258> [29 de noviembre de 2015]

68. OCDE. 2002. Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales. [en línea] <http://www.oecd.org/sti/ieconomy/15590267.pdf> [consulta: 29 de noviembre de 2015]

69. OCDE. 2006. Report on the cross-border enforcement of privacy laws. [en línea] <http://www.oecd.org/sti/ieconomy/37558845.pdf> [consulta: 24 de enero de 2016]

CONGRESOS.

70. DESANTES, José. 1991. El derecho fundamental a la intimidad. En: Seminario El derecho a la intimidad y a la vida privada y los medios de comunicación social: 28 de agosto de 1991. España, Centro de Estudios Públicos.

71. PÉREZ LUÑO, Antonio. 1990. Del habeas corpus al habeas data. En: Conferencia XIV Curso de Informática y Derecho: 11 de mayo de 1900. Toledo, Centro Regional de la UNED.

72. RÍOS, Lautaro. 1984. La dignidad de la persona en el ordenamiento jurídico español. En: XV Jornadas Chilenas de Derecho Público: 19 al 21 de octubre de 1984. Valparaíso, Universidad de Valparaíso, Facultad de Ciencias Jurídicas, Económicas y Sociales.

TESIS.

73. CERDA, Alberto. 2003. La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales. Tesis para optar al grado de Magíster. Santiago, Universidad de Chile. Escuela de Derecho.

LEYES NACIONALES.

74. CHILE. Ministerio de Justicia. 1925. Constitución Política de la República. 5 de octubre, 1971. [en línea] <http://www.leychile.cl/Navegar?idNorma=241203> [consulta: 24 de enero de 2016]

75. CHILE. Ministerio de Justicia. 1980. Constitución Política de la República. 22 de septiembre, 2005. [en línea] <http://www.leychile.cl/Navegar?idNorma=242302> [consulta: 24 de enero de 2016]

76. CHILE. Ministerio de Justicia. 1999. Ley 19.628: Sobre protección a la vida privada. 28 de agosto, 1999. [en línea] <http://www.leychile.cl/Navegar?idNorma=141599> [consulta: 24 de enero de 2016]

77. CHILE. Ministerio de Justicia. 2001. Ley 19.733: Sobre libertades de opinión e información y ejercicio del periodismo.

BOLETINES NACIONALES.

78. CHILE Cámara del Senado. 2009. Boletín N° 6.594-07: Proyecto de reforma constitucional que crea una Agencia de Protección de Datos Personales. 3 de julio, 2009.

79. CHILE. Cámara del Senado. 2010. Boletín N° 6.994-07: Restringe uso de determinados datos personales existentes en internet. 16 de junio, 2010.

80. CHILE. Cámara de Diputados. 2012. Boletín N° 8.143-03: Modificaciones a la Ley 19.628, sobre Protección a la Vida Privada y Protección de Datos de Carácter Personal. 11 de enero, 2012.

81. CHILE. Cámara de Diputados. 2014. Boletín N° 9.460: Modifica ley N° 19.733, sobre Libertades de Opinión e Información y Ejercicio del Periodismo, con el objeto de consagrar expresamente a los diarios electrónicos, como medios de comunicación social. 15 de julio, 2014.

82. CHILE. Cámara de Diputados. 2014. Boletín N° 9.461-19: Modifica sobre Libertades de Opinión e Información y Ejercicio del Periodismo, para exigir a los diarios electrónicos, el cumplimiento de las exigencias establecidas, para los medios de comunicación social. 15 de julio, 2014.

83. CHILE. Cámara del Senado. 2014. Boletín N° 9.384-07: Consagra el derecho a la protección de datos personales. 11 de junio, 2014.

LEYES ESPAÑOLAS.

84. ESPAÑA. Cortes Generales. 1979. Constitución Española. 29 de diciembre, 1978. [en línea] <http://boe.es/buscar/doc.php?id=BOE-A-1978-31229>[consulta: 24 de enero de 2016]

85. ESPAÑA. Jefatura de Estado. 1982. Ley Orgánica 1/1982: de protección civil del derecho al honor, a la intimidad personal y familia y a la propia imagen. 5 de mayo, 1982. [en línea] <https://www.boe.es/buscar/doc.php?id=BOE-A-1982-11196>[consulta: 24 de enero de 2016]

86. ESPAÑA. Ministerio de Relaciones con las Cortes y de la Secretaría del Gobierno. 1993. Real Decreto 428/1993: por el que se aprueba el Estatuto de la Agencia de Protección de Datos. 4 de mayo, 1993.

87. ESPAÑA. Jefatura de Estado. 1999. Ley Orgánica 15/1999: de Protección de Datos de Carácter Personal. 14 de diciembre, 1999. [en línea] <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750> [consulta: 24 de enero de 2016]

88. ESPAÑA. Jefatura de Estado. 2002. Ley 34/2002: de Servicios de la sociedad de la información y de comercio electrónico. 22 de julio, 2002.

[en línea] <https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758>[consulta: 24 de enero de 2016]

89. ESPAÑA. Ministerio de Justicia. 2007. Real Decreto 1720/2007: por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos de carácter personal. 19 de abril, 2008. [en línea] <https://www.boe.es/buscar/act.php?id=BOE-A-2008-979> [consulta: 24 de enero de 2016]

BOLETINES ESPAÑOLES.

90. PRIETO, María Jesús. 2004. Objeto y naturaleza jurídica del derecho fundamental a la protección de datos personales (I), Boletín del Ministerio de Justicia Español N°58.

FALLOS NACIONALES.

91. CHILE. Corte de Apelaciones de Santiago. Lusik con Martorell, Causa Rol N° 983-1993.

92.CHILE. Corte Suprema. 2012. Figueroa Silva con Prefecto de la Prefectura Cautín, Causa Rol N° 5.322-2012.

93.CHILE. Corte Suprema. 2015. Venegas Yáñez con Álvarez Marchant, Causa Rol N° 9.973-2015.

94.CHILE. Tribunal Constitucional. 2011. Causa Rol N° 1.984-2011.

FALLOS ESPAÑOLES.

95.ESPAÑA. Tribunal Constitucional. 1983. Sentencia N ° 22/1984.

96.ESPAÑA. Tribunal Constitucional. 1984. Sentencia N° 114/1984.

97.ESPAÑA. Tribunal Constitucional.1989. Sentencia N° 37/1989.

98.ESPAÑA. Tribunal Constitucional.1991.Sentencia N° 197/1991.

99.ESPAÑA. Tribunal Constitucional. Sentencia N° 151/1997.

100.ESPAÑA. Tribunal Constitucional. 2001. Sentencia N° 139/2001.

RESOLUCIONES ESPAÑOLAS

101.ESPAÑA. AEPD. Procedimiento de tutela de derechos N° TD 815/2012.

102.ESPAÑA. AEPD. Procedimiento de tutela de derechos N° TD 1558/2012.

103.ESPAÑA. AEPD. Procedimiento de tutela de derechos N° TD 2047/2012.

104.ESPAÑA. AEPD. Procedimiento de tutela de derechos N° TD 2086/2012.

105.ESPAÑA. AEPD. Procedimiento de tutela de derechos N° TD 1912/2013.

106.ESPAÑA. AEPD. Procedimiento de tutela de derechos N° TD 878/2015.

107.ESPAÑA. AEPD. Procedimiento Sancionador N° PS 2/2010.

108.ESPAÑA. AEPD. Procedimiento Sancionador N° PS 764/2010.

109.ESPAÑA. AEPD. Procedimiento Sancionador N° PS 337/2011.

110.ESPAÑA. AEPD. Procedimiento Sancionador N° PS 434/2011.

111.ESPAÑA. AEPD. Procedimiento Sancionador N° PS 446/2011.

112.ESPAÑA. AEPD. Procedimiento Sancionador N° PS 174/2012.

113.ESPAÑA. AEPD. Procedimiento Sancionador N° PS 449/2012.

114.ESPAÑA. AEPD. Procedimiento Sancionador N° PS 595/2012.

115.ESPAÑA. AEPD. Procedimiento Sancionador N° PS 210/2014.

116.ESPAÑA. AEPD. Procedimiento Sancionador N° PS 620/2014.

117.ESPAÑA. AEPD. Procedimiento Sancionador N° PS 721/2014.

ARTÍCULOS DE PERIÓDICOS ELECTRÓNICOS.

118.AGUIRRE, Francisco. 2014. Facebook "manipula" emociones de casi 700 mil usuarios y desata la polémica. [en línea] La Tercera en internet. 30 de junio, 2014. <http://www.latercera.com/noticia/tendencias/2014/06/659-584708-9-facebook-manipula-emociones-de-casi-700-mil-usuarios-y-desata-la-polemica.shtml>[consulta: 29 de noviembre de 2015].

119.AREYUNA, Héctor. 2014. Espionaje web: "Tener expectativa de privacidad en internet es un error". [en línea] Diario Uchile en internet. 30 de enero, 2014. <http://radio.uchile.cl/2014/01/30/espionaje-web-tener-la-expectativa-de-privacidad-en-internet-es-un-error>[consulta: 29 de noviembre de 2015].

120.DEMIDOVA, Nadezhda. 2014. Social network frauds. [en línea] Securelist en internet. 11 de junio, 2014.

<https://securelist.com/analysis/publications/63855/social-network-frauds/>[consulta: 29 de noviembre de 2015].

121. En las redes sociales no hay ninguna expectativa de tener privacidad. [en línea] El Diario Montañés en internet. 19 de febrero, 2015. <http://www.eldiariomontanes.es/sociedad/201502/19/redes-sociales-ninguna-expectativa-20150219003559-v.html>[consulta: 29 de noviembre de 2015].

122. Facebook espía tus conversaciones de WhatsApp, según Avast, [en línea] ABC Tecnología en internet. 30 de octubre, 2015. <http://www.abc.es/tecnologia/redes/abci-whatsapp-facebook-espia-conversaciones-whatsapp-segun-avast-201510301733_noticia.html> [consulta: 29 de noviembre de 2015]

123. Facebook: estas son las condiciones que aceptas sin leer. [en línea] 24Horas en internet. 11 de febrero, 2014. http://www.24horas.cl/tendencias/tecnologia/facebook-estas-son-las-condiciones-que-aceptas-sin-leer-1071759> [consulta: 29 de noviembre de 2015].

124.FRÍAS, Álvaro. 2009. Twitter no es una red social, es para todo el mundo sepas qué haces al momento. [en línea] El Mundo en internet. 26 de marzo, 2009.

125.FRY, Jason. 2010. Why Twitter looks like a social network but feels like new media. [en línea] NiemLab en internet. 7 de mayo, 2010. <http://www.niemanlab.org/2010/05/why-twitter-looks-like-a-social-network-but-feels-like-news-media/>[consulta:06 de noviembre de 2015]**.**

126.JIMÉNEZ, Rosa. 2012. Facebook deja al descubierto mensajes privados. [en línea] El País en internet. 25 de septiembre, 2012. http://tecnologia.elpais.com/tecnologia/2012/09/24/actualidad/1348507026_917653.html [consulta: 29 de noviembre de 2015].

127.PAGLIERY, José. 2015. Dos juegos para Android roban contraseñas de Facebook. [en línea] CNN en internet. 9 de julio, 2015. <http://cnnespanol.cnn.com/2015/07/09/dos-juegos-para-android-roban-contrasenas-de-facebook/#0>[consulta: 29 de noviembre de 2015].

128. Robadas 250.000 cuentas de Twitter. [en línea] El País en Internet. 4 de febrero, 2014. <http://tecnologia.elpais.com/tecnologia/2013/02/04/actualidad/1359967398_800973.html>[consulta: 29 de noviembre de 2015]