



Universidad de Chile
Facultad de Derecho
Departamento de Ciencias Penales

**USO, ABUSO Y MANIPULACIÓN PARA INCIDIR EN LOS PROCESOS DECISORIOS:
APROXIMACIÓN AL PARADIGMA DEL PROCESAMIENTO DE LA INFORMACIÓN EN
LA WEB PARA INFERIR LA PERSONALIDAD DEL USUARIO**

Memoria presentada a la Facultad de Derecho de la Universidad de Chile para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales.

Profesor Guía: Germán Ovalle Madrid

Memoristas:

Karina Cid Calderón

Karyna Ramírez Herrera

Santiago, Chile

2021.

RESUMEN

En la era de las tecnologías, dentro de las principales problemáticas que presenta la estructuración del proceso de toma de decisiones por parte de un individuo, corresponde a la posibilidad de trazar o realizar un seguimiento hacia el origen y los fines de la información por él percibida. De igual manera y a la inversa, una vez que el sujeto, de manera consciente o no, entrega su información personal, resulta tremendamente complejo realizar el seguimiento de a qué destinatario y con qué fines, se transmitirán o recepcionarán estos datos entregados. El presente Proyecto de Memoria de Tesis intenta indagar en los ejes claves a tener en cuenta para el discernimiento del proceso entre el uso y tratamiento de datos y de qué manera aquello puede constituir un abuso y manipulación sobre los mismos. Para ello se analizarán las principales plataformas de redes sociales actuales, los tipos de datos que es posible discriminar al amparo de la legislación nacional y cómo el avance de las neurociencias está influyendo en la manera de concebir el presente y perfilarnos hacia el futuro. En un mundo en que se está construyendo la identidad del individuo conciliando su vida civil con su desenvolvimiento en el mundo virtual, se vuelve cada vez más importante el cuestionar nuestras bases normativas en mira hacia el futuro.

A nuestras familias, amigos y docentes.

A todos quienes nos han acompañado en esta larga travesía con su fortaleza, humor, paciencia y cariño. Nos han inspirado más allá de lo que nuestras palabras pueden transmitir.

También, en un lugar muy hondo de nuestros corazones, a nuestras mascotas, nuestros más leales *roomies*, los que están y los que han partido.

Y a ti especialmente, mi compañera memorista, ya son años de hermandad y profesión. Pudimos, podemos y podremos todo.

Infinitas gracias.

TABLA DE CONTENIDOS

INTRODUCCION	6
CAPITULO I. DE LOS DIVERSOS TIPOS DE INFORMACIÓN EN LA WEB.	8
I. Clasificación de los tipos de información:	10
Personal- Pública.	10
Personal - Discreta.	11
Personal- Confidencial.	13
II. Teorías de la propiedad de la información: Restrictiva y Liberal.	13
Teoría Restrictiva	14
Teoría Liberal.	¡Error! Marcador no definido.6
CAPITULO II. DE LA ACTIVIDAD EN LA WEB, EL SEGUIMIENTO DE LA HUELLA DEL USUARIO Y LAS RESPONSABILIDADES ASOCIADAS.	18
I. Relación virtual: Conceptos y definiciones previas.	18
Usuario de Internet	18
Los prestadores de servicios	18
Los proveedores.	19
Los Operadores de Telecomunicaciones.	20
II. Redes sociales en línea.	22
III. Contratos en las redes sociales.	27
Registro	28
Condiciones o Términos de uso.	28
Sanciones	30
IV. Cláusulas de Exención de responsabilidad.	30
Limitación de la responsabilidad.	30
Exención de responsabilidad.	31
V. La actividad pública (Twitter)	32
Persona privada que utiliza su cuenta de Twitter.	33
Persona pública que utiliza una cuenta de Twitter institucional.	34
Persona pública que utiliza su cuenta de Twitter privada	36
VI. La actividad en ámbitos semicerrados (Facebook)	39
Exoneración de responsabilidad por medio de un contrato de adhesión y política de privacidad.	40
Uso de datos personales y tratamiento de la información de los usuarios en Facebook	¡Error! Marcador no definido.3

El negocio publicitario de los datos personales de los usuarios de Facebook; **Error! Marcador no def**

CAPITULO III. PROCESAMIENTO DE LA INFORMACIÓN EN LA WEB: USO Y TRATAMIENTO.

46

I. Conceptos clave.	46
Privacidad digital.	¡Error! Marcador no definido.6
Autodeterminación informática.	¡Error! Marcador no definido.7
Tipos de datos.	¡Error! Marcador no definido.8
II. El ámbito de lo permitido conforme a la normativa vigente.	49
A.- Resolución de Madrid	51
B.- Marco Normativo Ley 19.628	¡Error! Marcador no definido.5
¡Error! Marcador no definido.	56
ii) Ámbito de aplicación de la Ley 19.628	56
III. El ámbito de lo permitido conforme a la voluntad explícita y tácita	¡Error! Marcador no definido.8
Libertad en el tratamiento de datos en Chile	¡Error! Marcador no definido.8
El consentimiento	59
Derechos del titular de datos personales.	61

CAPITULO IV. EL PROBLEMA DEL PROCESAMIENTO Y SU USO PARA INCIDIR EN LOS PROCESOS DE DECISIÓN:

63

I. Problema:	
a. Etapas del tratamiento de datos	63
b. Mecanismo de control	63
c. Transmisión de datos a terceros	65
d. Actores del mercado de datos personales	66
II. Uso para incidir en procesos de decisión económica	67
a. Datos personales de carácter económico, financiero, bancario o comercial	67
b. Datos necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.	69
III. Uso para fines electorales	70
a. Mercado de datos personales públicos	70
b. Mercado de datos personales en internet	71
IV. La respuesta desde la combinación de aspectos de temas a abordar: Las neurociencias, la neuroética y los neuroderechos.	72
a. Las neurociencias	73
b. La neuroética	75
c. Los neuroderechos	76

CAPITULO V. LO AFECTADO DESDE LA TEORÍA DEL BIEN JURÍDICO	80
I. Los riesgos de no regular	80
II. La posible necesidad de una intervención del derecho penal. Hacia una regulación global.	81
III. La manipulación de los procesos decisorios y la contravención a la garantía constitucional de configurar libremente el plan de vida (la dirigibilidad de la conciencia y los procesos decisorios)	85
CONCLUSIONES	88
BIBLIOGRAFÍA	91

INTRODUCCION

“En el pasado, eras lo que tenías ahora eres lo que compartes”.

Godfried Bogaard

La configuración de la identidad digital a raíz de la incorporación de las redes sociales ha puesto hincapié en la dicotomía que se produce para el individuo, toda vez que las realidades se ven interpuestas unas con otras. El *mundo real* comienza a difuminar sus límites con el *mundo informático* y con ello se abren distintos escenarios en los cuales nos tendremos que desenvolver. En este sentido, los procesos de información (entrega de datos, recopilación, tratamiento, uso, transacción, etc.) toman fundamental relevancia ya que permiten la entrada de terceros ajenos a los ámbitos privados y confidenciales de los usuarios de la web, utilizando para ello la huella digital que éstos han dejado (consciente e inconscientemente) al momento de navegar por internet.

Si el paradigma que significa la intromisión recién mencionada fuese unidireccional, es decir, que la información que circula en la web fuese solo aquella que como usuario estoy dispuesto a entregar de forma voluntaria, no veríamos obstáculo alguno. Lamentablemente, lo cual configura justamente la propuesta de este trabajo, nos encontramos hoy en día ante una realidad diametralmente opuesta. La injerencia y popularización de las redes sociales vía internet, entre ellas, Facebook, Twitter, Instagram, etc., han transformado la personalidad virtual de los usuarios en una especie de moneda de cambio, susceptibles de ser transables y cuantificables desde el punto de vista económico. Así las cosas, nos encontramos en presencia de un mercado de datos personales, en el que paradójicamente el usuario se considera una fuente de información sobre sus propios datos pero quienes lucran con ellos resultan ser terceros agentes en el sistema, quienes vuelven difusa la intencionalidad originaria con que el individuo presta su consentimiento, más o menos compelido a ello, por la propia dinámica de las plataformas.

Nuestro propósito en el presente Proyecto de Memoria es visibilizar el uso y abuso que ocurre en el tratamiento de los datos personales, estudiando la situación desde las

diversas aristas que se requieren para poder dar un entendimiento más completo en la materia, partiendo por considerar al individuo en su aspecto dual de titular de su información personal, como a la vez usuario de plataformas y servicios tecnológicos, revisando las problemáticas que representan para esta dicotomía, temáticas claves como la voluntad, el ejercicio de la libertad, la posibilidad de realizar una autodeterminación identitaria, tanto en el mundo real como digital, las implicancias en materia de responsabilidad e irresponsabilidad de los agentes del sistema, la dinámica del conocimiento necesario para dar acabada protección a la voluntad del sujeto, la transmisión de sus datos, distinguiendo el origen de sus fuentes, y los fines con que terceros utilizan esta información, la preocupante incidencia y posible manipulación, a la luz y evaluación crítica de todos los factores mencionados, de nuestros procesos decisorios en cuanto usuarios reales, seres humanos a quienes les asisten una serie de garantías y derechos que, según podremos observar, el alcance de su resguardo parece ser insuficiente según el avance de las tecnologías de la información, vertiginoso por lo demás, pero al cual el Derecho pareciera observar desde lejos.

Abarcaremos además los ámbitos innovadores dentro de este acercamiento entre el Derecho y las tecnologías de la información, estudiaremos las neurociencias, las neurotecnologías y los neuroderechos, así como sus regulaciones generales y sectoriales, a la vez que su incidencia dentro del Derecho Penal de manera específica y dentro del Ordenamiento Jurídico en su concepción general.

Invitamos al lector a realizar un viaje exploratorio por las vías del Derecho y la actualidad tecnológica, a sumarse a nuestras inquietudes y quizás, esperamos, se cuestione junto a nosotras esta realidad que a veces parece estar dada, ser estática, y donde las bases de nuestras construcciones jurídicas se sienten ya inamovibles. Todo en pos del permanente crecimiento y revisión crítica al que debe estar sujeto el Derecho, puesto que es en la revisión de sí mismo, de su entorno y de sus actos, en que el individuo puede propender a dar un salto evolutivo, tanto social, normativo e individual y acercarse de una mejor manera a la realidad que a veces todos observamos desde diversas aristas pero que se nos escapa en una revisión más global. Como bien dicen, a veces hay que alejarse del árbol para poder ver el bosque.



Con un solo clic en el botón que se muestra en la imagen, la información que sea registrada por el usuario de internet pasará a formar parte de la web y contribuirá (de manera consciente o inconsciente) con sus datos personales, gustos, preferencias, intereses, hábitos, política, religión, sexualidad, etc., a la construcción de su perfil digital, el que a grandes rasgos se conoce como *identidad digital* o *personalidad virtual*.

Así, esta huella o marca personal del usuario en la web será utilizada por la llamada *sociedad de la información*, denominada así por la convergencia a que da origen las telecomunicaciones y la informática, aprovechando que “los perfiles así creados permiten a los prestadores de servicios de la sociedad de la información enviar, a los usuarios, publicidad específica dirigida a ellos”¹, aquella que se conoce como “publicidad online comportamental”².

El escenario que se presenta ante el usuario de la web, indica que por un lado existe una incipiente manifestación de voluntad y, por otro lado, que muchas veces terceros ajenos a este proceso decisorio utilizan información en ausencia de su voluntad por medio del tratamiento de la huella digital que ha dejado en su paso por la web.

Lo anterior nos hace replantearnos algunos temas ¿Toda la información que proporcionamos en la web puede ser tratada y usada por terceros? ¿Existe un límite en

¹ Navas, S. (01 de marzo de 2015). La personalidad virtual del usuario de internet. *Centro de Estudios de Consumo*. p. 1. <https://blog.uclm.es/cesco/files/2015/03/La-personalidad-virtual-del-usuario-de-internet-.pdf>

² La publicidad online comportamental (Online Behavioural Advertising) se refiere a una nueva forma de publicidad que tiene su fundamento en los intereses y comportamiento de los usuarios. Se trata de un rastreo temporal de la navegación de los usuarios para hacerles llegar publicidad de acuerdo a la huella digital que estos han dejado en la web.

su tratamiento o es libertad de comunicación pura versus el derecho a la intimidad que tenemos como seres humanos? Para poder responder estas preguntas, primero debemos comenzar por entender cuál es el escenario en que nos encontramos actualmente y cómo confluyen los distintos espacios de nuestras vidas frente a la creación de una especie de personalidad virtual: individual y social³.

Tradicionalmente los seres humanos nos encontramos ante la dicotomía constante de determinar qué es lo que corresponde a nuestro ámbito privado, íntimo y público. Comprendiendo que estos tres ámbitos “se situaban desde el núcleo de la personalidad hacia afuera”⁴. No obstante, lo anterior, si observamos el funcionamiento de las redes sociales y su incidencia en las personas, nos vamos a encontrar ante un movimiento distinto en la forma de percibir como confluyen estos tres ámbitos, donde su punto de partida es lo externo, es decir, desde afuera hacia el núcleo de la personalidad. Y, es más, ya no es la persona la que se encuentra en esa constante dicotomía para determinar qué es lo que corresponde a cada ámbito, adquiriendo un rol más pasivo en este proceso decisorio, en el que inconscientemente cada vez que hace un clic, otorga el poder de decisión a un tercero, quien va a determinar por la persona que es lo que corresponde a su vida privada, íntima y pública.

En efecto, los avances tecnológicos, y con ello las redes sociales han venido desarticulando los conceptos de privacidad, intimidad y publicidad. Y ello, en opinión de Emilio Suñé Llinás ha provocado “una importante tensión entre dos grandes valores: libertad de información y protección de la intimidad y demás derechos y libertades fundamentales frente a ella, sobre todo cuando se dispone de datos muy abundantes sobre las personas, gracias a los sistemas informáticos, y se emplean a fondo las posibilidades que éstos dan”⁵. Así las cosas, encontrándonos ante esta realidad desarticulada “lo que hace la red social es convertir la esfera de lo privado en público, debido a que todo lo que se publique en ella no está regido por el concepto de

³ La personalidad virtual, individual y social, son conceptos que serán abordados con mayor análisis en el capítulo dos del presente trabajo, a saber: Capítulo II: “De la actividad en la web, el seguimiento de la huella del usuario y las responsabilidades asociadas”.

⁴ Jaramillo, O. (2010). La desarticulación de lo público y lo privado en las redes sociales. *Las audiencias activas, nuevas formas de participación pública. Consideraciones éticas y jurídicas*, p.48. ISBN 970996206X.

⁵ Suñé, E. (2002). *Tratado de Derecho Informático* (Vol.1). Madrid, España: Universidad Complutense Madrid. p.16.

confidencialidad, por lo que de inmediato se pierde la autodeterminación informativa”⁶. Esto quiere decir que le ha ido restando voz a la persona en este proceso decisorio y reduciendo finalmente el ámbito de lo íntimo a lo secreto. Con el objetivo de profundizar en las ideas desarrolladas en este párrafo, los próximos dos subcapítulos abordarán el estudio de los distintos tipos de información que se encuentran disponibles en la web y cuáles son las teorías que se manejan sobre su propiedad.

I. Clasificación de los tipos de información:

Antes de comenzar a clasificar los distintos tipos de información que se encuentran disponibles en la web, el primer alcance que debemos hacer es acotar el tema en revisión para efectos de encauzar su estudio a lo que nos convoca, es decir, nos vamos a centrar en analizar la información personal de los usuarios en la web. Dicho de otra manera, este primer subcapítulo va a tratar de la información personal y sus clasificaciones.

Personal- Pública.

Según lo planteado por Jaramillo:

"La información de carácter personal que está en las redes sociales proviene de cinco fuentes básicas: el mismo usuario que entrega información de manera voluntaria, otros usuarios de las mismas redes sociales que publican información sobre nosotros, empresas asociadas y no asociadas a las redes sociales que recolectan información sobre nosotros, la misma red social que registra y procesa información sobre nuestras actividades y, por último, los motores de búsqueda (buscadores) que indexan los perfiles y los ponen a disposición de cualquier usuario de Internet”⁷.

En este orden de ideas, y frente a la amplia cantidad de información que se maneja en la web sobre los usuarios, sería contraproducente negar que estamos frente a dos conceptos (Personal- Público). Los cuales a primera vista parecen ser contrarios, pero que a raíz de este proceso de desarticulación de los ámbitos privados y públicos por la

⁶ Jaramillo, op. cit. p.8.

⁷El Economista América.com. (29 de agosto de 2016). *El Economista América*. <https://www.economistaamerica.cl/telecomunicacion-tecnologia-cl/noticias/7790793/08/16/Redes-sociales-los-limites-de-lo-publico-y-lo-privado.html>

inserción de las redes sociales (que ya mencionamos), realmente no son opuestos, sino que, por el contrario, vienen a formar una categoría o clasificación especial a la luz de esta nueva personalidad virtual, individual y social del usuario de internet. Que nos llevaría a encontrarnos, ya no frente a esa dualidad (Personal-Público) sino que nos vamos a mover derechamente en la esfera de lo personal, y que, desde ahí, se van a originar estas subclasificaciones: información personal e información personal pública.

Si analizamos la información personal en sí, hay dos conceptos que son fundamentales para su entendimiento, estos son: Autodeterminación y confidencialidad. Ambos conceptos se refieren a la persona en sí misma, y por ello, podríamos suponer que es ella quien decide el uso de su propia información, pero lo que ocurre realmente es que estamos frente a una suposición que es aparente, ya que “lo que hace la red social es convertir la esfera de lo personal en público, debido a que todo lo que publique en ella no está regido por el concepto de confidencialidad”⁸. Así las cosas, entendemos que el concepto de información personal pública nace mediante la visualización en la web de la información personal de los usuarios, su tratamiento y su utilización. Es decir, las redes sociales entienden que, por el simple hecho de *publicar* una foto, subir un comentario, compartir un like, dar me gusta a un producto, registrarse en una página web, etc., sería el mismo usuario de internet quien transformaría la información (la que en un comienzo era personal) en una información personal que será pública. Este proceso en el cual se ve envuelto el usuario de la red, lo estudiaremos con mayor detención en el próximo capítulo, pero nos parece correcto adelantar que tendrá consecuencias directas en la formación de responsabilidades desde el punto de vista ético y penal.

Personal - Discreta.

La información personal de los usuarios de internet, que en un comienzo permanecía en el ámbito privado, se ha trasladado de escenario y en reiteradas ocasiones se han confundido sus límites. Justamente por ello es que hay campañas de concientización de la población usuaria de la web, con el objeto de que aprendan a delimitar claramente hasta qué punto están dispuestos a entregar información personal suya.

El autor Alberto Cerda opina que:

⁸ El Economista, Loc. cit.

“el desarrollo de los medios de comunicación evidenció la insuficiencia del derecho a la intimidad como simple expresión de ámbitos de exclusión a la injerencia de terceros, e hizo patente la necesidad de ampliar la protección que brindaba a su titular, para permitir que este pudiese disponer de control sobre la información personal que le compete”⁹.

Por ello, ya no podemos entender a la privacidad desde el punto de vista clásico de lo público y lo privado, estamos hablando de una dimensión distinta, que sigue siendo privacidad, pero abarca aquella parte extensiva y pública que viene de la mano de las redes sociales. Esta se denomina *autonomía individual* y se refiere a “la capacidad de elegir, de tomar decisiones informadas, en otras palabras, a mantener el control sobre diferentes aspectos de nuestra propia vida”¹⁰.

En este orden de ideas, es en esta dimensión extensiva y pública de la privacidad, donde el individuo discriminará sobre el tipo de información personal que considera factible hacer pública y cuál prefiere mantener de forma discreta. La información personal discreta abarca todo aquello que el individuo considera necesario mantener al resguardo y parcialmente visible, decidiendo qué, cómo, cuándo y quién podrá acceder a ella. Otorgándole así una valoración emocional distinta y, por ende, limitando su contenido disponible. Podemos señalar que la autonomía individual en este escenario infinito que es la web necesariamente tiene que adaptarse y es así como nace la *autodeterminación informativa*. Esta adaptación,

“implica necesariamente poderes que permitan a su titular definir los aspectos de su vida que no sean públicos que desea que se conozcan, así como las facultades que le aseguren que los datos que de su persona manejan informáticamente terceros son exactos, completos y actuales y que se han obtenido de modo leal y lícito. También supone el control sobre el uso de esa información ya que ésta en sí

⁹ Del Fierro, C. (2018). *Derecho al olvido ante los servicios de búsqueda en internet*. Santiago, Chile.[Memoria para optar al grado de Licenciado en Ciencias Jurídicas, Universidad de Chile]. p. 48. Citando a Cerda, A. (2012). *Legislación sobre protección de las personas frente al tratamiento de datos personales*. Centro de Estudios en Derecho Informático. p. 7.

¹⁰ Del Fierro, Loc. cit. Citando a Terwagne, C. (2012). *Privacidad en Internet y el derecho a ser olvidado/derecho al olvido*. Revista de Internet, Derecho y Política. p. 54. http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-terwagne_esp/n13-terwagne_esp

misma no tiene ninguna utilidad si no es para ser utilizada en múltiples relaciones”¹¹

Personal - Confidencial.

Es fácil cometer el error de confundir el concepto de confidencialidad con el de privacidad. Lo anterior ocurre, ya que se encuentran relacionados el uno con el otro, pero es su espacio en la vida de la persona la que los diferencia. Esto quiere decir que mientras la privacidad se manifiesta en la parte interna del individuo, la confidencialidad apunta a sus acciones. En este sentido, podríamos entender como información confidencial a los datos cuyo contenido considera o revela antecedentes que, para su titular, de manera expresa e intencional, busca que se mantenga parte de su esfera privada, ya que desea mantener en reserva.

Llevando la confidencialidad a las redes sociales (y relacionándolo con el punto anterior), primero debemos dejar en claro que es parte de la esfera de la información personal de los usuarios y que su manipulación, tanto por el mismo usuario como por terceros ajenos, la vuelve vulnerable y penetrable. Por ello, para mantener dicha información en el carácter de confidencial se requeriría de una administración consciente del usuario de internet y de un manejo y una difusión ética y responsable de aquellos que acceden a ella.

Lamentablemente, la confidencialidad, así como la planteamos, desde un punto de vista ético y responsable, no se encuentra cabalmente regulada por los ordenamientos jurídicos, solo existen atisbos de ella y se encuentra subsumida en algunos derechos como, por ejemplo, el derecho a la intimidad. De hecho, paradójicamente se le entrega una responsabilidad adicional al usuario de internet, ya que constantemente se le hacen recomendaciones para, entre otras, disminuir la difusión de su información confidencial.

II. Teorías de la propiedad de la información: Restrictiva y Liberal.

“Mientras otros ganan acceso a nuestra información (especialmente cuando no se da el consentimiento para la recolección o no nos enteramos de ello), perdemos

¹¹ Del Fierro, op. cit. pp.48-49. Citando a Murillo, P. (1993). *Informática y protección de datos personales*. Madrid: Centro de Estudios Constitucionales. p.32.

poder y control. Debido a la accesibilidad y durabilidad de la memoria digital, el poder de la información no solo se desplaza del individuo a la contraparte conocida, sino que también a terceras partes desconocidas. Esto solidifica y profundiza las existentes diferencias de poder entre los info-ricos y los info-pobres, y puede incluso denegarle a los individuos sus propias concepciones sobre su pasado.”¹²

En este subcapítulo, analizaremos algunas ideas sobre la propiedad de la información, en donde nos vamos a referir a dos teorías: La teoría restrictiva y a la Liberal.

De acuerdo a lo desarrollado en los párrafos anteriores, podemos indicar que la idea de un titular de la información que circula en la web ha sido y sigue siendo un tema controversial, que hasta el día de hoy no tiene una postura única. Ya que si bien, se encuentra reconocida la titularidad del usuario sobre su información y datos personales, no ocurre lo mismo con su propiedad y todos los derechos que ello conlleva. Lo anterior queda en evidencia, toda vez que,

“el usuario de internet, siendo titular de su información personal, pierde prácticamente el control sobre ella ya que quien lo ostenta y, por tanto, tiene el poder económico sobre la misma, son terceros ajenos al usuario de internet (v. gr. editores de sitios web, anunciantes, redes de proveedores de publicidad, etc....). Además, el control sobre esta información es asimétrico provocado por los propios titulares de cookies o tecnología similar”¹³.

La información que se encuentra en la web, tuvo un emisor original, que a simple vista se puede entender como el titular de dicha información. Pero al ser plasmada en la web, su dominio se vuelve difuso y comienzan a tomar relevancia otros participantes de esta red social. Así las cosas, pasaremos a analizar en este apartado, dos teorías que buscan darle respuesta a esta inquietud.

Teoría Restrictiva.

¹² Del Fierro, op. cit. p. 45. Citando a Mayer-Schönberger, V. (2009). Delete: The Virtue of Forgetting in the Digital Age. Princeton: Princeton University Press. p. 69.

¹³ Navas, op. cit p.1.

Para poder entender aquello que se denomina como *información informática* (dentro de la cual se incluye los datos personales) y la importancia que tiene el poder determinar su titularidad o propiedad, consideramos necesario comenzar por explicar que,

“en términos generales, cosa es todo lo que tiene entidad, ya sea corporal o espiritual, natural o artificial, o real o abstracta, y que tiene cualidades que la diferencian de las demás. Es decir, se trata de todo aquello que existe y que ocupa un espacio en la realidad. Esta a su vez, puede ser de tres maneras: a) Física o material. Corresponde a las cosas que se encuentran ubicadas en la tercera dimensión y que son perceptibles por los sentidos. b) Intelectual. Se trata de las ideas, las cuales son creadas y percibidas por la razón humana. Estas aparecen en virtud de un proceso cognoscitivo de creación y pueden estar o no basadas en la realidad. c) Virtual. Es una categoría intermedia entre las dos anteriores, pero con características propias. En ella se involucran elementos intelectuales que son perceptibles por los sentidos, especialmente la vista y, en algunos casos, a través de comandos de voz, en la medida en que los elementos informáticos son puestos en funcionamiento por la interacción que el individuo ejerce directa o indirectamente sobre ellos”¹⁴.

Entonces, cuando hablamos de información informática estamos en presencia de una cosa o bien, la que en vista de los artículos 565 y 576 del Código Civil chileno¹⁵ siendo incorporal tiene la calidad de un derecho, ya sea real o personal.

Este bien incorporal presenta diferentes características, entre ellas y quizás una de las más importantes la enuncia Miguel Ángel Davara al indicar que,

“es un bien que no se agota con su consumo y que puede ser utilizado por muchas personas al mismo tiempo, sin que por ello se cause ningún daño o perjuicio al propio bien que, posiblemente, sea favorable a múltiples intereses distintos para los que se produjo, lo anterior, se explica porque una vez que los costos iniciales de generar y “producir” la información se contraen, los usos adicionales se pueden emprender a un costo marginal relativamente bajo. De hecho, publicistas, instituciones financieras y compañías de seguros pueden usar la misma

¹⁴ León, E. (2006). La posesión de los bienes inmateriales. *Revista de Derecho Privado*. pp. 77-116. <https://www.redalyc.org/articulo.oa?id=360033184002>

¹⁵ El artículo 565 del Código Civil de Chile, reza así “Los bienes consisten en cosas corporales o incorporales. Corporales son las que tienen un ser real y pueden ser percibidas por los sentidos, como una casa, un libro. Incorporales las que consisten en meros derechos, como los créditos, y las servidumbres activas”. Además el artículo 576 del Código Civil de Chile señala que “Las cosas incorporales son derechos reales o personales”

información comercial y cooperar en su generación, aun cuando cabe señalar que, si bien estos actores utilizan la misma información, la naturaleza del uso es bastante distinta. De este modo, podemos concluir que la información ha ido asumiendo cada vez más, la particularidad de ser un bien económico”¹⁶

Con lo recién señalado, no queremos confundir al lector, efectivamente la información y los datos personales se han transformado en bienes económicos, transables en el mercado. Pero siguen manteniendo la característica fundamental de que son intrínsecos a la persona, y ello es innegable. Por dicho motivo, parte de la doctrina simpatiza aun con la idea de que la información digital de los usuarios de la web sigue siendo un bien intransable e intangible, por lo cual no sería factible comercializar su propiedad ya que se encontraría en la categoría de bien personal, entregando con ello su propiedad única y exclusivamente al mismo usuario, sin distinguir, además, entre la diferenciación que se hace actualmente entre titularidad y propiedad.

Teoría Liberal.

“Al final quién toma las decisiones acerca del mejor uso a dar a la información personal no es su titular sino un tercero, el cual, puede llegar a obtener ingentes beneficios negociando con la información personal de los usuarios, a cambio de un precio, en un “mercado secundario”, si bien debería ser el titular de esa información quién decidiera libremente el uso más conveniente a dar a la misma, esto es, qué datos personales concretos permite que usen terceros de forma gratuita o a cambio de una contraprestación. (...) Esto implica un cambio en la configuración de la información personal. Se trata de un recurso más que se puede llegar a tener una explotación económica relevante. Jurídicamente la información personal debería considerarse un “bien intangible” sobre el cual el usuario, titular de la misma, tiene poder de disposición”¹⁷

¹⁶ Jervis, P. (2006). *La Regulación del Mercado de Datos Personales en Chile*. [Tesis para optar al grado de Magíster en Derecho, Universidad de Chile]. p. 28. Citando a Davara, M (1996). *De las autopsias de la información a la sociedad virtual*. Pamplona. Editorial Aranzadi S.A. p. 50.

¹⁷ Navas, op.cit. p. 2.

En este orden de ideas, y ya entendiendo que la cosificación de la información digital es un hecho irrefutable, que al individuo se le reconozca su propiedad y ya no solo su titularidad no debería ser un obstáculo, sino muy por el contrario, deberíamos estar en presencia de una garantía. Ya la información y los datos personales dejaron de tener la característica de “indisponibles”. Esto ocurrió desde que se diferenció la titularidad de la información personal de la propiedad de la misma, siendo absolutamente necesario disponer de aquellas facultades que son intrínsecas a ella. La teoría liberal se hace cargo (dentro de lo posible) de armonizar el interés social por el uso y tratamiento de la información, con la posibilidad de que en este mercado de datos personales, el usuario pueda percibir las ganancias que le corresponderían por su información. Volviendo de esta manera a ubicar al usuario de la relación virtual, en un agente activo y ya no meramente pasivo de su huella digital.

CAPITULO II. DE LA ACTIVIDAD EN LA WEB, EL SEGUIMIENTO DE LA HUELLA DEL USUARIO Y LAS RESPONSABILIDADES ASOCIADAS.

A lo largo de este capítulo, iremos analizando la forma en que se va manifestando la existencia de la huella digital que los usuarios de internet van dejando a medida que navegan por la web y su incidencia en distintos escenarios, como por ejemplo las redes sociales en línea, el contrato de suscripción o adhesión y la disyuntiva de la responsabilidad/ irresponsabilidad. Esto entendiendo que simplemente al conectarnos a internet se va a producir una situación en que distintos participantes de la red van a generar un vínculo (en algunos casos contractual, y en otros, extracontractual), pero que debido a la compleja arquitectura de internet muchas veces puede ser difícil de visualizar quien realmente forma parte de esta relación virtual y quien es el tercero ajeno a ella.

I. Relación virtual: Conceptos y definiciones previas.

En este sentido, consideramos necesario definir brevemente algunos conceptos que nos permitirán establecer un primer acercamiento a esta compleja relación virtual. A saber: Usuario de internet, prestador de servicios, proveedores y los operadores de telecomunicaciones¹⁸.

Usuario de internet.

Si bien existen diferentes definiciones para el concepto de usuario, consideramos que la enunciada por la autora Lydia Esteve González reúne la generalidad y la especialidad del concepto. La autora señala que “los usuarios de Internet son todas aquellas personas físicas o jurídicas, profesionales, estudiantes, consumidores, empresas u organismos que acceden a Internet, y a sus aplicaciones”¹⁹.

Los prestadores de servicios.

¹⁸ Hacemos presente al lector que en internet se pueden producir distintos tipos de relaciones o vínculos virtuales, y que los participantes de estas, pueden ser algunos de los mencionados u otros.

¹⁹ Aravena, C. y De la Fuente, O. (2010). *Régimen Contractual de las Redes Sociales en Internet*. Santiago, Chile. [Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile]. pp. 247-248. Citando a Esteve, L. (2006). *Aspectos Internacionales de las infracciones de derechos de autor en Internet*. Editorial Comares. España. p. 109.

Debido a que esta categoría resulta demasiado amplia, consideramos primeramente que, se requiere identificar el rol que juega el prestador de servicios en esta relación virtual para luego conceptualizarlo. No obstante, lo anterior, y siguiendo a la autora González serían “todos aquellos intervinientes que prestan algún servicio, cualquiera que sea, por medio o en relación con Internet”.²⁰

Los proveedores.

Para definir a estos participantes del vínculo virtual ya mencionado, consideramos que una conceptualización general es suficiente, ya que serán clasificados de acuerdo al tipo de servicio que desempeñen. Por tanto, un proveedor según la RAE se entiende como “Dicho de una persona o de una empresa: Que provee o abastece de todo lo necesario para un fin a grandes grupos, asociaciones, comunidades, etc.”

Tratándose en definitiva de los vínculos que potencialmente se van a generar con los usuarios de internet, podemos distinguir: 1. Los proveedores de internet o ISP (Internet Service Provider) pueden ser definidos como “empresas que, si bien pueden dedicarse a variadas funciones, se ocupan de uno u otro modo de prestar servicios de acceso y conexión a Internet. Son quienes ponen a disposición de los usuarios los medios técnicos necesarios para realizar su conexión.”²¹ y, 2. Los proveedores de información o de contenidos: Aquellos que,

“ponen a disposición del usuario el depósito o lugar que sirve de medio de almacenamiento de información y posibilita la interacción entre los participantes del servicio. Los proveedores de contenidos en este caso, se identifican efectivamente con la red social y más específicamente con la persona encargada de la administración del servicio, pudiendo tomar la forma de personas jurídicas o bien de sujetos particulares, indistintamente.”²²

²⁰ Aravena, C. Loc.cit. Citando a Esteve, L. Loc. cit.

²¹ Aravena, C. op.cit. p. 249.

²² Aravena, C. op.cit. p. 250.

Los Operadores de Telecomunicaciones.

Se entiende por operadores de telecomunicaciones “aquellos que transmiten información, y funcionan de puente entre el Proveedor de Acceso a Internet y el usuario.”²³ Su rol en este vínculo o relación virtual recae en la transmisión de la información, siendo un eslabón más de estos participantes “aunque en la realidad, la mayoría de las veces su persona va a coincidir con la del Proveedores de Acceso a Internet o ISP.”²⁴

En este mismo orden de ideas, y ya conceptualizados los principales participantes de la relación virtual, nos parece relevante detenernos frente a dos de estos participantes, a saber: los usuarios y los prestadores de servicios. Ello, pues el papel que desarrolla el usuario de internet, es primordial para analizar la huella o rastro digital que queda en la web toda vez que navega en búsqueda de distintas informaciones o por diversos objetivos, ya sean de comunicación, ocio, entretenimiento, cultura, compras etc.

Algunos autores han considerado que el rol del usuario de internet en este proceso de conexión sólo se remite a *buscar* pero tal como vimos en el capítulo anterior, a medida que va obteniendo la información se va produciendo una especie de intercambio, que consciente o la mayoría de las veces inconscientemente, ocurre cuando las diferentes páginas de internet consultadas retienen la información proporcionada por el usuario (almacenan los rastros de su huella digital). Y finalmente, este usuario que en un principio era solamente un *buscador* se convierte en una fuente digital de su propia información haciendo clic a un me gusta, a una noticia, a una compra de un objeto en particular, etc. va generando un perfil digital. El que prontamente los proveedores utilizarán los datos proporcionados por los mismos usuarios para distintos fines²⁵ (sean estos lícitos o no). Así las cosas, el usuario de internet deja ese rol asignado de buscador y cambia continuamente al de informante, donde la moneda digital de cambio, a sabiendas suya o no, es su propia información.

²³ Aravena, C. op.cit. p. 253.

²⁴ Aravena, C. Loc. cit.

²⁵ Véase el capítulo IV “El problema del procesamiento y su uso para incidir en los procesos de decisión”.

Es importante señalar que este vínculo de navegación o conexión precisa de un funcionamiento determinado y debe cumplir con normativas de uso. En este sentido se ha indicado que,

“Todos los ordenadores de Internet, ya sean servidores o usuarios, tienen que estar identificados de alguna forma. Y para ello se utiliza la dirección IP²⁶: cuatro números del 0 al 256 separados entre sí por un punto; por ejemplo, 185.47.814.2. Internet es una red y, como toda red, ha de trabajar con un determinado protocolo de transmisión de datos, que indica cómo se efectúa la transferencia de información entre los computadores de la red. El protocolo utilizado por Internet se llama TCP/IP (Transmisión Control Protocol / Internet Protocol). La dirección IP es la información mínima que proporciona cualquier usuario al conectarse a Internet”²⁷.

En virtud de lo expuesto y a nuestro juicio, nos encontramos ante una nueva forma de digitalización en la web que se refiere al aspecto social del usuario de internet. Ya analizamos en el párrafo anterior la forma en que la huella digital del usuario al momento de navegar por la red, va dejando rastros y lineamientos, con los cuales se construye por terceros su personalidad virtual individual. Ahora nos corresponde desarrollar la idea del aspecto social del usuario de internet.

Esta personalidad virtual social, es un concepto construido por medio de las relaciones e interacción de las siguientes ideas, el de personalidad virtual y el del aspecto social del usuario de internet, por ello si bien no existe una definición como tal, podríamos dar un primer paso o acercamiento a su conceptualización señalando que se entiende por personalidad virtual social aquel perfil que el usuario de internet configura y exhibe a través de las redes sociales en línea²⁸.

Nos parece pertinente que antes de profundizar en las dos redes sociales en línea que son parte del estudio de este capítulo (Facebook y Twitter) primero debemos entender qué es una red social. Si señalamos que los usuarios de internet “navegan e interactúan

²⁶ Las siglas IP provienen de la frase Internet Protocol, que traducido al español significa Protocolo de Internet. Este protocolo se encarga de establecer las comunicaciones en la mayoría de nuestras redes, para ello se asigna una dirección única e inigualable a cada dispositivo la cual se utilizará para identificar cada dispositivo dentro de una red.

²⁷ Cabezas, P. y Moya, F. (2008). *El derecho al anonimato del usuario de internet*. Santiago, Chile. [Memoria para optar al grado de Licenciado en Ciencias Jurídicas, Universidad de Chile]. p. 18.

²⁸ Concepto que analizaremos en los próximos párrafos antes de profundizar en las dos redes sociales en línea que se estudian en este capítulo, Twitter y Facebook.

no sólo con los sitios, sino también con los demás usuarios, con ello se forma lo que se ha denominado como comunidades o “redes sociales”²⁹. Actualmente nos encontramos frente a diferentes redes sociales, entre las cuales adquieren un valor de estudio trascendental las redes sociales en línea.

II. Redes sociales en línea.

Si bien podemos encontrar diferentes definiciones de redes sociales en línea, para efectos de este trabajo, nos interesa entregar un concepto que nos permita introducir los próximos ítems a estudiar (Twitter y Facebook), por ello las entendemos como estructuras sociales que comprenden grupos indefinidos de personas que comparten intereses de forma común y que se ven continuamente manifestados por medio de distintos canales digitales, donde finalmente se estructura una identidad digital.

Estas estructuras sociales a las que nos referimos, le permiten al usuario de internet desarrollarse ya no solo en un plano individual, sino que además social. Los perfiles que los usuarios de internet construyen a raíz de sus intereses, objetivos, gustos, ideologías, cultura, etc., son expuestos ante la comunidad de la red, donde la privacidad y la publicidad se encuentran en una pugna constante y que en muchas ocasiones cede ante los requerimientos de lo social por sobre lo privado.

Justamente en este punto debemos detenernos para analizar cómo el funcionamiento de estas redes sociales en línea, que le dan cabida al aspecto social de los usuarios de internet, comienzan a cavar profundamente en la personalidad virtual individual y terminan finalmente por dejar expuesto ante terceros (cuyos fines de utilización de datos personales pueden o no ser lícitos) al usuario de internet, desvalorizando sus derechos, algunos tales como el derecho a la intimidad, a la libertad de expresión e información, entre otros.

Junto con la exposición social del usuario de internet, otros participantes de esta relación virtual comienzan a tener una mayor participación. De hecho, estas especies de *carpetas digitales de los usuarios* construidas a través del uso y tratamiento de sus datos personales junto con la huella digital que ha dejado en la web, es vendida a empresas

²⁹ Cabezas, P. op.cit. p. 14.

privadas (otras veces a organismos estatales) que consideran este tipo de información de un valor comercial mayor a lo que pagan por ello. Sus objetivos para utilizar dichos datos, son variados, pueden ir desde la simple captación comercial a una forma de control estatal. Es tan diversa la forma en que la información de un usuario puede ser utilizada, que incluso en muchas ocasiones se encuentran al límite de lo lícito, pudiendo ser utilizada incluso en contra del propio usuario al momento por ejemplo de una entrevista de trabajo, pues se pudo haber efectuado un estudio suyo mediante el personal de Recursos Humanos y que se haya encontrado justamente una publicación antigua, con su nombre, en donde su actuar no se condice con los principios y políticas de la empresa. Es aquí donde la conocida frase coloquial que dice “tu pasado te condena”, tiene una directa incidencia y como estamos hablando de las redes sociales en línea, ese *pasado virtual* jamás será pasado, vivirá en la red y será utilizado para diferentes fines. Ya que la propiedad de esa información, si bien directamente no es de la web, su uso y tratamiento si lo es.

Se ha considerado que el usuario tiene, ante esta y otras situaciones de indefensión, distintos derechos que puede utilizar con el objetivo de retomar de alguna manera el control sobre su huella digital presente en la web, estamos hablando de los derechos “ARCO”.

La legislación, tanto internacional como nacional, ha considerado que el usuario de internet ha visto menoscabada su personalidad virtual, individual y social ante el tratamiento y uso de su huella digital por parte de las grandes empresas privadas (tras aquellas conocidas redes sociales en línea, entre otras) y el control estatal que ejerce el estado valiéndose en diferentes ocasiones de los datos personales recabados de sus ciudadanos. Por lo anterior, y tal como lo ha indicado Vergara a lo largo del desarrollo de su investigación:

“se han reconocido al usuario los siguientes derechos: De acceso, rectificación, cancelación y oposición. Se ha señalado que el derecho de acceso permite solicitar y obtener información acerca de si sus datos personales están siendo tratados por el responsable y acceder a ellos, en su caso. El derecho de rectificación busca que se modifiquen o completen los datos cuando sean inexactos o incompletos. El derecho de cancelación persigue que se supriman o eliminen los datos del titular por las causales previstas en la ley. El derecho de

oposición permite requerir que no se lleve a cabo un tratamiento de datos determinado por la concurrencia de las causales previstas en la ley”³⁰

La búsqueda del reconocimiento legal de estos derechos del usuario digital, vienen necesariamente de la mano con sus características de gratuidad e irrenunciabilidad, pues a fin de “asegurar un buen ejercicio de los derechos ARCO, se establece un procedimiento directo y eficaz para que cualquier titular de datos pueda recurrir directamente ante el responsable de datos, ejerciendo el correspondiente derecho ARCO, permitiéndose bloquear transitoriamente los datos en cuestión”³¹. En Chile, nuestra legislación ha señalado que si el responsable del tratamiento de los datos, dentro del plazo en que el usuario ha realizado la solicitud ejerciendo alguno de los derechos ARCO ya mencionados, no la responde dentro del plazo que establece la ley para ello o no acoge, de plano, su solicitud, el usuario seguirá teniendo la posibilidad de recurrir a dos instancias posteriores, que son: presentar un reclamo ante la correspondiente autoridad de control y, en aquellos casos de disconformidad con la resolución, podrá recurrir ante la respectiva Corte de Apelaciones.

Como veremos en los próximos capítulos del presente trabajo, nuestra legislación nacional ha presentado importantes avances en el tratamiento de datos personales y también respecto al reconocimiento de los derechos virtuales que tienen los usuarios de internet. No siendo nuestro objetivo el desmerecer dichos avances, sí debemos señalar que existen tareas pendientes y que es necesario regular prontamente el reconocimiento que otras legislaciones internacionales le han otorgado a nuevos derechos y figuras jurídicas a favor de los usuarios digitales. A modo de ejemplo, podemos mencionar que “se introduce el derecho a la portabilidad de los datos personales, en virtud del cual el titular de datos puede solicitar y obtener del responsable en un formato electrónico estructurado, genérico y de uso habitual, una copia de sus datos personales y

³⁰Vergara, M. (2017). Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales (Vol. 6, Número 2). *Universidad de Chile*. pp. 135-152. <https://doi.org/10.5354/0719-2584.2017.45822>

³¹ Se recomienda la lectura del Boletín N°11.144 (2007). Proyecto de ley, iniciado en mensaje de S. E. Presidenta de la República. *Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales*.

comunicarlos o transferirlos a otro responsable de datos”.³² También se ha dado una atención especial al denominado derecho al olvido, con la intención de reforzar su importancia y necesidad de regulación, sobre todo con ocasión de aquellas infracciones penales, civiles, administrativas y disciplinarias que se cometen a raíz del tratamiento de los datos personales de los usuarios y la huella digital que estos van dejando en la web. Se podría decir que el derecho al olvido “busca equilibrar adecuadamente el derecho de las personas a reducir el acceso a información desfavorable y que afecta su reputación social, con el derecho a la información y el interés público que hay envuelto en el acceso a ella”³³.

Tanto, en los derechos ARCO como en los derechos a la portabilidad y al olvido, se han implementado diferentes medidas o campañas de concientización, algunas impulsadas por los organismos estatales y otras, por las mismas empresas privadas que compiten por la mayor captación de usuarios en la web. El objetivo de ellas, es establecer que ya no es el usuario (al hacer clic y adherirse a las condiciones de uso y políticas de un sitio web) quien debe ser el responsable de aquella huella digital suya en la web, sino que se debe centrar la responsabilidad en el tercero que los trata, es decir que ahora la atención se centra en el momento de utilizar los datos personales.

Esta nueva perspectiva, si bien cambia el foco de atención al darle relevancia a la hora de responsabilizar por el uso de datos personales a los que los tratan, no tiene la intención de desconocer que el usuario digital, como titular de sus datos personales, ejerza su deber de información. De hecho, se señala que “la falta de conciencia ciudadana respecto al uso de los datos personales que no se ciñe, únicamente, a aspectos de ciberseguridad. Existe una carencia generalizada respecto al conocimiento de cómo los datos personales serán tratados adecuadamente, según su finalidad y propósito”³⁴.

Por ello, el consentimiento, sigue siendo la principal fuente de legitimidad del tratamiento de los datos personales. Y para que este sea válido, debe ser informado, libre, inequívoco, otorgado previamente al tratamiento y específico en cuanto a sus fines. Si

³² Boletín N°11.144 (2007). Proyecto de ley, iniciado en mensaje de S. E. Presidenta de la República. *Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales*. p. 14.

³³ Boletín, op.cit. p.7.

³⁴ Cuaderno de trabajo N° 13 (2019). Democracia y Protección de Datos Personales en la Era Digital. *Consejo para la transparencia*. p.19.

hablamos de las redes sociales, este consentimiento tendrá además un apellido informado. Se ha conceptualizado el consentimiento informado como aquel acto que ocurre antes de obtener el consentimiento final de usuario, donde se explica al individuo de investigación lo que se va a hacer con sus datos, quién tendrá acceso a ellos y cómo van a ser publicados. Esta es una medida concreta que busca empoderar al usuario y titular del uso y tratamiento de su propia información, para que reconozca y ejerza su autodeterminación digital.

Este enriquecimiento digital denominado autodeterminación, junto con reformar la idea del consentimiento del uso y tratamiento de los datos personales, crea una especie de decálogo que busca regular los deberes y obligaciones de quienes son responsables del tratamiento de datos. Entre algunos de ellos podemos mencionar, el deber de confidencialidad, la licitud del tratamiento de datos en sí mismo, deber de reserva, el deber de información, medidas de seguridad, etc. Junto con lo anterior, también señala excepciones a las reglas del consentimiento, entre las que nos parecen relevantes, por ejemplo, aquellos casos cuando la recolección de la información proviene de una fuente de acceso público, si proviene de una obligación de carácter legal, si son datos de obligaciones comerciales, bancarias, etc.

Así las cosas, la autodeterminación digital establece una serie de medidas, estas son:

“1. El individuo es el centro del sistema de recolección, gestión y uso de datos. 2. El individuo decide qué información revelar, de forma selectiva. 3. Control sobre los fines para los que se usan los datos, así como su duración, a través de contratos. 4. El individuo tiene mecanismos para comunicar lo que demanda de forma abierta y flexible, sin estar ligado a ninguna organización concreta. 5. Altas medidas de seguridad. 6. Portabilidad de datos, de modo que los individuos puedan obtener todos sus datos y moverlos de un proveedor de servicios a otro. 7. Medidas para que las empresas sean responsables de la seguridad de los datos personales, de acuerdo a los distintos niveles de permiso que el individuo ha decidido otorgar”³⁵.

Todo lo anterior evidencia que el propósito de que las legislaciones, nacional e internacional, es el de no imponer cargas excesivas que hagan compleja la circulación de

³⁵ Cuaderno, op.cit. p. 17. citando a Rubinstein en Gil (2016). p. 141.

la información en la web, lo que realmente busca es ya no sean las empresas (sean estas, de carácter privado o público, entendidas como cualquier organismo destinado a recolectar y guardar datos personales de los usuarios) quienes dispongan de la huella digital de los usuarios a su arbitrio sino que cumplan con estándares de cuidado y responsabilidad en el uso y tratamiento de la información personal de los usuarios de internet, que estos estándares sean diferenciados, según sea una persona natural o jurídica (incluso órganos del estado), que indiquen claramente cuáles serán sus objetivos al tratar los datos, regular la cesión o transferencia de las bases de datos, entre otros. De hecho,

“una de las principales innovaciones de esta nueva normativa es la regulación del tratamiento automatizado de grandes volúmenes de datos, o “Big Data”, protegiendo la facultad de control del titular sobre su propia información, pero reconociendo también la licitud del acceso y uso de la información por parte de terceros y particularmente, de las empresas”³⁶.

En este punto de la investigación consideramos necesario analizar un acto específico que es aplicable a la mayoría de las redes sociales en línea, la contratación. Ello ya que cuando hablamos de consentimiento informado y de autodeterminación digital, sería el estándar ideal de cultura que podrían alcanzar los usuarios de internet, pero que a raíz justamente de este tipo de contratación, queda demostrado que aún existe un desconocimiento al respecto (de hecho, muchas veces se desconoce que se encuentran ante un tipo de contrato en la web) y que dicho estándar de conocimiento se encuentra en transición.

III. Contratos en las redes sociales.

Cuando nos referimos a los contratos de las redes sociales, estamos considerando un conjunto de tipos contractuales distintos, siendo el más estudiado (y el que desarrollaremos de forma más acabada) el contrato de suscripción. En estas circunstancias, se nos presenta un primer cuestionamiento a este tipo de contrato ¿realmente nos encontramos ante un contrato?

³⁶ Cuaderno, op.cit. p.19.

Tal como señala el Código Civil chileno en su artículo 1438, el “Contrato o convención es un acto por el cual una parte se obliga para con otra a dar, hacer o no hacer alguna cosa. Cada parte puede ser una o muchas personas”. Luego, el profesor López Santa María entiende al contrato como “un acto jurídico bilateral o convención que crea obligaciones”³⁷. Conforme a estas definiciones, el contrato de suscripción de las redes sociales, podría calificarse como tal, toda vez que,

“son contratos que se celebran entre el sitio y los usuarios, razón por lo que dicha calificación es correcta. En efecto, existen derechos y obligaciones para ambas partes. El sitio ofrece al usuario las funcionalidades de la red social de que se trate y se obliga a cumplir con las condiciones de usabilidad y políticas de privacidad. De su parte el usuario se compromete a no efectuar las conductas reprochables y catalogadas en el reglamento de la red social”³⁸.

En el mismo orden de ideas, y complementando la definición anterior, podemos señalar que

“tiene por objeto el prestar un servicio a través de las diversas aplicaciones en Internet, el cual consiste básicamente en el tratamiento de datos por parte del sitio en favor de los usuarios, permitiendo así relacionar la información de los usuarios con otros, fomentando la interactividad entre ellos gracias a sus diversas aplicaciones o utilidades. Los servicios variarán según las propias políticas y motivaciones con las que se formó, mantenga y opere el sitio”³⁹.

A continuación, realizaremos un breve análisis de los elementos principales de los contratos de suscripción a las redes sociales, los que, si bien no son iguales, mantienen un formato básico o estándar de aplicación:

Registro.

El que se lleva a cabo por el usuario de internet al completar un formulario con sus datos personales solicitados por el sitio al cual se quiere suscribir. En este sentido, se considera

³⁷ López, J. (1998). *Los Contratos Parte General*. (2º ed., Vol. 1). Santiago, Editorial Jurídica de Chile. p. 15.

³⁸ Aravena, C. op.cit. p.115.

³⁹ Aravena, C.op.cit. p. 119.

que la *identificación del usuario* es la mínima condición de seguridad, tanto para el propio usuario, como para el sitio y los demás usuarios de internet.

Condiciones o Términos de uso.

Cada red social, de acuerdo a su política e interés de desarrollo, establece “condiciones o términos de uso”, para regular principalmente tres aspectos. Estos son: El uso del sitio web, la interacción del usuario de internet y la convivencia entre ellos.

Estas construcciones establecidas para controlar la conducta de los usuarios,

“se relacionan en términos generales, con el clásico paradigma que señala que los derechos de un sujeto terminan en donde comienzan los derechos de los demás. En base a ello, es que se puede identificar cuatro grandes principios que rigen el ámbito de control establecido en las redes sociales en Internet. Estos son los siguientes: - Protección a la figura del menor de edad (...)- La búsqueda de información veraz, oponiéndose a la simulación o falsa identidad de los usuarios, correos electrónicos y en general, cualquier otro tipo de dato relativo a la identidad. - Prohibición en algunos sitios de la divulgación, difusión o publicación de material pornográfico, pedófilo, zoofilia o de otras conductas reprochables dentro del ámbito de la sexualidad. - Prohibir en general cualquier tipo de publicación difamatoria, desagradable, vulgar, ofensiva o dañosa en sí misma, sea cualquiera su formato, texto, imagen, videos, nickname de usuarios y cualquier otra forma de manifestación”⁴⁰.

Cabe mencionar, que, si bien nos parece adecuado que existan condiciones y regulaciones por parte de los sitios web, lo que se nos presenta contradictorio y finalmente deja en un estado de indefensión al usuario de la red, es que se suprime la libertad y la manifestación de voluntad de éste, toda vez que adhiere o acepta automáticamente las condiciones o términos de uso con solo un clic. La imagen a continuación habla por sí sola, el usuario para poder acceder, utilizar o ser partícipe del sitio web al que se está suscribiendo debe aceptar y estar de acuerdo con su política de términos y condiciones. Esta aceptación total y automática, pone en jaque el real sentido de la manifestación de voluntad que debe existir en todo contrato y genera a la larga, distintos tipos de problemas, algunos de ellos dicen relación con los usos comerciales y

⁴⁰ Aravena, C. op. cit. p. 50.

finés publicitarios con que los sitios web manejarán los datos personales de sus usuarios, entre otros.



Tus datos personales se utilizarán para procesar tu pedido, mejorar tu experiencia en esta web y otros propósitos descritos en nuestra [política de privacidad](#).

He leído y estoy de acuerdo con los [términos y condiciones](#) de la web *

Realizar el pedido

Sanciones.

Todo sitio web establece en sus condiciones o términos de uso, un apartado especial para aquellos comportamientos de sus usuarios que son considerados faltas o sanciones. Y cuyos efectos pueden ser diversos, aunque los más conocidos son: Eliminación de lo publicado por el usuario en el sitio web, suspensión o eliminación temporal de la cuenta del usuario y finalmente, el bloqueo permanente de la cuenta.

IV. Cláusulas de exención de responsabilidad.

Según Díez-Picazo señala que al hablar de responsabilidad nos estamos refiriendo a “la sujeción de una persona que vulnera un deber de conducta impuesto en interés de otro sujeto a la obligación de reparar el daño producido”⁴¹. Así las cosas, podemos comprender que el nacimiento de la responsabilidad va a ocurrir ante un hecho que genera daño y esto nos hace preguntarnos ¿existe un sistema de responsabilidad cuando hablamos de internet y de sus redes sociales?

Ante la pregunta recién formulada, y ya analizados los anteriores elementos del contrato de suscripción, podemos visualizar dos conductas diferentes de los sitios web, pero relacionadas la una con la otra. La primera es la limitación de la responsabilidad y la otra, su exención.

Limitación de la responsabilidad.

⁴¹ Díez-Picazo, L. y Guillón, A. (1989). *Sistema de Derecho Civil*. (Vol. II). Tecnos. p. 591.

Siendo la limitación de la responsabilidad penal una cláusula especial dentro de estos contratos de suscripción. Podemos señalar que:

“nos encontramos con disposiciones expresas en los contratos, términos o condiciones de uso, los que al ser establecidos por los sitios y aceptados por los usuarios, son vinculantes y obligatorios para ambas partes. Los sitios de redes sociales en Internet establecen, con respecto a la responsabilidad, un conjunto de disposiciones comunes (...). Con todo, las disposiciones comunes que se pueden encontrar sirven de guía en cuanto al tratamiento general de responsabilidad en los sitios de redes sociales de Internet, así como enseñan cuáles serán los intereses específicos que se pretenden cautelar.”⁴².

Lo recién señalado, demuestra que, si bien los sitios web establecen disposiciones comunes de responsabilidad, su interés es delimitar el daño que se pudiera causar a usuarios o terceros, con el fin de responder sólo en aquellos casos en que sus condiciones o políticas de uso lo establezcan.

Exención de responsabilidad.

Por otro lado, se ha señalado que,

“los sitios excluyen su responsabilidad en cuanto a posibles daños cuando sean producidos por el uso del servicio, del sitio Web o de los contenidos publicados en él (...) Esta generosa recopilación de cláusulas de responsabilidad - o más bien su exclusión de responsabilidad -, presenta lo que se mencionó como una exención general de responsabilidad a favor de la red social, permitiendo sostener que la regla general consiste precisamente en la exención total de responsabilidad ante cualquier hecho dañoso que ocurra con motivo de la utilización del servicio que las redes sociales prestan ya sea que se generen daños a usuarios o terceros”.⁴³

A grandes rasgos podemos mencionar que estas cláusulas de responsabilidad, tal como se indica en el párrafo anterior, son verdades exenciones de ella. Lo que nos hace encontrarnos de frente con la denominada disyuntiva de la “responsabilidad/irresponsabilidad”. Esto quiere decir que el límite del estándar de responsabilidad es tan difuso, que produce dos efectos: primero, el que sea casi imposible o muy dificultoso que un sitio web se responsabilice, por ejemplo, sobre las acciones o publicaciones que

⁴² Aravena, C. op.cit. p. 63.

⁴³ Aravena, C. op. cit. p. 66.

realizan sus usuarios (en especial de aquellas que son difamatorias e injuriosas), de daños que se produzcan con ocasión de sus servicios o que de ellos se afecte publicaciones, equipos, datos o archivos, tanto de sus propios usuarios como de terceros ajenos al sitio, de la violación del derecho a la imagen o del derecho de propiedad intelectual, entre otros. Y el segundo efecto se refiere a aquellos casos en que los sitios web y las empresas (privadas o públicas) se hacen responsables por el mal uso y tratamiento de los datos personales sean la excepción. Ya que, por medio de estas cláusulas, que aparentan una intención de regular la responsabilidad, lo que realmente hacen es excluirse de ella, dejando “en un evidente estado de indefensión al usuario, quien no tendría en principio la posibilidad de perseguir la responsabilidad del sitio conforme a las disposiciones contractuales ya revisadas”.⁴⁴ En definitiva, el usuario de internet se encuentra constantemente en una posición desfavorable. Por un lado, acepta los términos y condiciones de uso del sitio web al cual se quiere suscribir y accede de esa manera a su contenido, o, por otro lado, se niega, y, por ende, queda excluido de uso.

A continuación, y luego de haber desarrollado la contratación como punto común entre los sitios web, desde la disyuntiva de la *responsabilidad/ irresponsabilidad*, procederemos a analizar la actividad del usuario de internet, por medio de su huella o rastro digital, tomando como principales referentes a Facebook y Twitter. Las formas en que la huella digital de los usuarios es determinada, guardada, recopilada y utilizada en las redes sociales en línea, son variadas y dependen de las condiciones de uso que le son informados al usuario al momento de suscribirse. Luego, el tratamiento de sus datos personales alcanza otros ribetes, en el que por medio de su información personal se intenta mantener un tipo de control sobre este.

V. La actividad pública (Twitter)

Tal como señalamos en los párrafos anteriores, Twitter es considerado como una red social en línea, tiene su origen el año 2006 y su creador es Jack Dorsey. Se puede definir como “una red de información que conecta en tiempo real a personas con otras personas o empresas, con las últimas noticias, opiniones e historias de su interés”⁴⁵.

⁴⁴ Aravena, C. op.cit. p. 68.

⁴⁵ Casado, C. (2017). Personalidad y preferencias de uso en las redes sociales en línea. *Universitat Ramon Llull. FPCEEB - Psicología*. p. 32. <http://hdl.handle.net/10803/409670>.

La forma en que Twitter comparte y distribuye la información en la web, ya sea proporcionada por sus propios usuarios o terceros, es mediante los tweets (mensaje de texto breve que no supera los 140 caracteres). A ello permite añadir etiquetas, hashtags, por medio de:

“palabras concatenadas seguidas de la almohadilla #. De esta manera, podemos acceder a noticias o a intereses personales o profesionales, buscando el hashtag por el buscador de Twitter, así como también etiquetar nuestros tweets para que aparezcan en las búsquedas y puedan comentar otros usuarios de la red con los mismos intereses. El uso de Twitter es básicamente informativo aunque su uso social también es importante ya que se puede buscar y seguir amigos y enviar mensajes privados”.⁴⁶

Los fines por cuales los usuarios utilizan esta red social en línea, es variada, incluso se ha extendido a ámbitos profesionales y de captación de empleos, donde empresas y personas naturales, utilizan esta red para dar a conocer su formación académica y experiencia laboral con el fin de que su perfil se haga interesante a los ojos de aquellos captadores de empleos.

Twitter, como red social en línea, se maneja en el ámbito público. Esto quiere decir que los usuarios que se suscriben a esta red social saben que sus publicaciones tendrán una visibilidad pública y que aquellas posibilidades de sus clientes para establecer espacios de privacidad son enumeradas. Ante este escenario, creemos que es pertinente hacer la siguiente distinción: Persona privada que utiliza su cuenta de Twitter, persona pública que utiliza una cuenta de Twitter institucional y persona pública que utiliza su cuenta de Twitter privada. Las tres perspectivas antes mencionadas, serán analizadas por medio de tres dictámenes del Tribunal Constitucional de Chile, saber: Dictamen N°14.953, año 2019, Dictamen N°18.671, año 2019, y Dictamen N° 6.696, año 2020.

Persona privada que utiliza su cuenta de Twitter.

Este es el escenario más común, en el que una persona ya sea natural o jurídica, crea una cuenta de Twitter y al momento de suscribirse a ella, por medio del correspondiente registro, adhiere a sus políticas de términos y condiciones de uso (esta situación la fuimos

⁴⁶ Casado, Loc.cit..

desarrollando de forma detenida en los párrafos anteriores a raíz del contrato de suscripción en las redes sociales).

En este sentido, es el usuario digital, quien, a través de su consentimiento informado, acepta expresamente unirse a una red social en línea determinada, ya habiéndose informado de las condiciones de uso del sitio web. En el caso particular de Twitter, es necesario revisar lo indicado en su política de términos y condiciones, donde expresamente se refiere a su funcionamiento, manejo de información de los usuarios y estándar de responsabilidad.

A grandes rasgos podemos indicar que Twitter, actúa de forma similar a las otras grandes redes sociales en línea, como lo son Facebook, Instagram, YouTube, entre otras, cuya tendencia ha sido limitar o disminuir notoriamente sus responsabilidades, mantener una política de uso de datos en que el usuario solo adhiere de forma expresa mas no consciente y donde quién recibe la mayor carga de responsabilidad es el mismo usuario. A modo de ejemplo podemos señalar que Twitter,

“no será responsable de la conducta online u offline de ningún usuario del sitio Web o del servicio. Esto incluye que el sitio no será responsable frente a ningún contenido, aplicaciones o software de terceros que sean publicados en el sitio por éste, por un usuario o bien por terceros a través de equipos o programas asociados al sitio o servicio. (...) además declara en sus términos que, si bien se arroga la facultad de regular a través de los términos y condiciones de uso las conductas, actividades y publicaciones de los usuarios, lo cierto es que no consideran realizar un control sobre estos de manera obligatoria, por lo que no serían responsables de lo que realicen sus usuarios”⁴⁷.

Persona pública que utiliza una cuenta de Twitter institucional.

Este otro escenario plantea, que una entidad pública para realizar publicaciones de carácter oficial sobre materias públicas atinentes a su cargo, debe utilizar los medios que son establecidos como oficiales por las correspondientes instituciones. Desde la Contraloría, ya se ha reconocido que es válido y permitido “el acudir al uso de tecnologías

⁴⁷ Twitter. (19 de agosto de 2021). *Twitter*. Recuperado el 8 de noviembre de 2021, de <https://twitter.com/es/tos>

de la información para apoyar la labor administrativa, postura que encuentra su fundamento en los principios de eficiencia y eficacia, transparencia y publicidad administrativas y debido cumplimiento de la función pública por parte de los organismos públicos (aplica el dictamen N° 43.233, de 2015, entre otros⁴⁸).

Debido a las denuncias ante el órgano contralor que interpusieron los señores Manuel Lobos González y David Zúñiga Vera, señalando que la Policía de Investigaciones de Chile (PDI) habría realizado una actividad irregular, bloqueando sus cuentas personales de la cuenta institucional, es que se dictó el dictamen N° 18.671, del año 2019. El referido dictamen se vale de diferentes normas constitucionales, entre estas, los artículos 5, 8 y 19 número 12 de la Constitución, con el objeto de plasmar que los órganos estatales, sus actos y procedimientos son de carácter público y que frente a ellos se asegura la libertad de todas las personas sobre sus opiniones e información, asegurando además su responsabilidad en caso de que dichos derechos no sean respetados. En tal sentido, se ha señalado por Contraloría, primero, que, a la luz de las nuevas tecnologías, los órganos de administración del estado pueden utilizar las redes sociales con el fin de mantener a la ciudadanía en constante información sobre las materias que le merezcan relevancia, de una forma eficaz, informada y oficial. En este sentido,

“dicha red virtual es un medio que pueden utilizar los organismos del Estado para dar a conocer a la colectividad usuaria de la misma hechos o acciones directamente relacionados con la consecución de sus fines y con su quehacer institucional, así como también de participación ciudadana en la gestión pública al ser de libre acceso, en cuanto a los usuarios y a las opiniones que en esa plataforma abierta se expresen, cumpliendo, por cierto, las reglas y términos del referido servicio de difusión”⁴⁹.

Por tanto, estas cuentas oficiales de las instituciones u organismos del estado, además de ser considerados canales directos de información pública, que dependen directamente del órgano público que representan, y ende, del estado. Deben cumplir, además, como cualquier otro usuario digital, con las normativas que el sitio web estipula en sus términos y políticas de uso, al momento de suscribirse a él.

⁴⁸ Dictamen N° 18.671. Lobos G., Manuel y Zúñiga Vera., David con la Policía de Investigaciones de Chile. (10 de julio de 2019). Contraloría General de la República de Chile.

⁴⁹ Dictamen, Loc. cit.

Persona pública que utiliza su cuenta de Twitter privada.

Este escenario, de persona pública que utiliza su cuenta de Twitter privada, lo estudiaremos de acuerdo a los dictámenes N° 14.953 y N°6.696, ambos emitidos por la Contraloría General de Chile los años 2019 y 2020, respectivamente. La materia denunciada es la siguiente:

“El señor Luis Hernández Olmedo denuncia que el Ministro de Relaciones Exteriores lo habría bloqueado en su cuenta personal de la red social Twitter, siendo ello improcedente, en su opinión, ya que se trataría de un recurso público y de un canal de acceso directo a los ciudadanos, no correspondiendo limitar arbitrariamente su utilización, solicitando además el listado de cuentas bloqueadas por aquél.”⁵⁰

A la luz de los hechos denunciados en el dictamen N°14.953 del año 2019, el órgano contralor manifestó su criterio, dando a entender que existe una diferencia entre las redes sociales en línea, tanto desde el punto de vista del usuario como de la cuenta que se utiliza. Así las cosas, una persona pública como lo es el Ministro de Relaciones Exteriores que tiene su cuenta personal de Twitter, puede utilizarla para los fines que considere necesarios y sean los convenidos entre la red social en línea y el usuario. Tomando ello en consideración, en una primera instancia, el órgano contralor ha manifestado que no correspondería su intromisión toda vez que ello,

“limitaría los derechos del titular sobre la misma y las políticas de usuario incorporadas en la relación jurídica existente entre una persona y la anotada red digital. Asimismo, hace presente que todos los contenidos que publicita esa Secretaría de Estado pueden encontrarse en la cuenta institucional de Twitter, siendo ésta de libre escrutinio para cualquier ciudadano que acceda a aquélla. Finalmente, agrega que carece de potestades legales para realizar acciones intrusivas en la aludida cuenta personal para la obtención de datos como los exigidos”.⁵¹

Para fundamentar su criterio recurre a la normativa constitucional señalando que el “artículo 19, N° 12, de la Constitución Política de Chile, asegura a todas las personas, la libertad de emitir opinión y la de informar, sin censura previa, en cualquier forma y por

⁵⁰ Dictamen N° 14.953. Hernández Olmedo, Luis., con Ministro de Relaciones Exteriores. (4 de julio de 2019). Contraloría General de la República de Chile.

⁵¹ Dictamen, Loc.cit.

cualquier medio, sin perjuicio de responder de los delitos y abusos que se cometan en el ejercicio de estas prerrogativas.”⁵² Y de acuerdo a ello, finalmente termina exponiendo su decisión, señalando que

“una cuenta de carácter privado de una persona en la citada red social, que ejerce como una autoridad de gobierno y que no afecta la probidad administrativa, por lo que queda dentro del ámbito particular de la misma, no corresponde que esta Contraloría General emita un pronunciamiento acerca de la posibilidad que aquella posee, como usuario, para bloqueos de otras cuentas o de su mantención.”⁵³

En virtud de lo anterior, podemos señalar que en esta primera instancia el órgano contralor se declaró incompetente para realizar acciones de intromisión en la cuenta personal de una persona pública, por entender dicha relación entre el usuario y la cuenta, de carácter privado. Luego, en una segunda instancia y a raíz de lo expuesto en el dictamen N°6.696 del año 2020, el criterio de la Contraloría toma un nuevo curso, al considerar un antecedente más: El contenido de la publicación.

Comienza el análisis del dictamen N°6.696 del año 2020, señalando que los hechos denunciados son los siguientes “el uso por parte de autoridades de la Administración del Estado de las cuentas personales que mantienen en redes sociales -en las que en algunos casos han bloqueado usuarios- para la comunicación de asuntos relativos a los organismos que dirigen”⁵⁴. A diferencia del dictamen anterior, esta vez el órgano contralor considera importante analizar el contenido de la información que se publica en esta red pública y social, desde una cuenta privada de una entidad pública. Para ello, es necesario hacer una mención a los dictámenes N°71.422, del año 2013 y al N°79.472 del año 2016, entre otros, donde se ha manifestado por el órgano contralor dos directrices: La primera, es que se puede “acudir al uso de tecnologías de la información para apoyar la labor administrativa, postura que encuentra su fundamento en los principios de eficiencia y eficacia, transparencia y publicidad administrativas y debido cumplimiento de la función pública por parte de los organismos públicos”⁵⁵, y la segunda, dice relación con que,

⁵² Dictamen, Loc. cit.

⁵³ Dictamen, Loc. cit.

⁵⁴ Dictamen N° 6.696. Uso de cuentas personales y bloqueo de usuarios. (23 de marzo de 2020). Contraloría General de la República de Chile.

⁵⁵ Dictamen N° 43.233. Fernández., Gene por Estatutos de Carabineros de Chile, feriados y uso de tecnologías. (1 de julio de 2015). Contraloría General de la República de Chile.

”la cuenta institucional en una red social de una entidad pública corresponde a un bien del organismo respectivo, que debe ser utilizado para servir a los fines institucionales o para publicitar comunicaciones o hechos de interés general para toda la población acerca de algún aspecto relevante de las labores, actividades o tareas que versen acerca de su funcionamiento, en correspondencia con el derecho de los ciudadanos a conocer y ser informados de las actividades y labores desarrolladas en forma continua y permanente por los servicios públicos”⁵⁶.

Estos dos criterios deben ir en directa relación con el contenido de la información que se publica por parte de personas públicas en cuentas personales en las redes sociales.

Lo antes expuesto, quiere decir que estamos frente al siguiente escenario: Cuando las entidades públicas aun disponiendo de cuentas institucionales, establecidas por los diferentes organismos públicos para informar a la ciudadanía de una manera oficial sobre una determinada materia, prefieren hacer uso de sus redes sociales privadas. En estas circunstancias, el órgano contralor ha señalado lo siguiente

“si la autoridad utiliza su cuenta personal para entregar información antes que la cuenta institucional o cuando la información obtenida en ejercicio del cargo es proporcionada únicamente a través de la cuenta privada, ella debe someterse a las mismas reglas de apertura, no discriminación, transparencia y publicidad que la cuenta del órgano público, encontrándose, en consecuencia, impedido el bloqueo de usuarios”⁵⁷.

Por tanto, la Contraloría, incorporando el nuevo elemento ya mencionado (el contenido de lo publicado), considera que sería por voluntad y consentimiento de la propia autoridad pública, que ésta “transforma su cuenta personal en una vía de comunicación pública de la información del ministerio, subsecretaría, servicio o municipalidad”⁵⁸. Esto quiere decir, que independiente de que la entidad pública utilice su cuenta de Twitter personal, si el contenido de lo publicado en ella, dice directa relación con información que ha obtenido a raíz de su cargo como personal administrativo del estado, será considerado que tal

⁵⁶ Dictamen N° 6.696. Uso de cuentas personales y bloqueo de usuarios. (23 de marzo de 2020). Contraloría General de la República de Chile.

⁵⁷ Dictamen, Loc. cit.

⁵⁸ Dictamen, Loc. cit.

información representa a los canales oficiales, y por ende, el control que el estado pueda ejercer sobre la cuenta personal de aquella entidad pública, no sería entendido como una violación a su derecho de privacidad, ni a otros derechos similares que puedan verse afectados por dicha intromisión.

VI. La actividad en ámbitos semicerrados (Facebook)

Luego, tenemos otra red social en línea, Facebook, la que fue creada por Mark Zuckerberg el año 2004 “con el objetivo de conseguir que el “mundo” fuera más abierto y estuviera conectado, en línea. La gente utiliza Facebook para estar conectada con sus amigos y familia; descubrir qué está pasando en el mundo y, por otro lado, para compartir y expresar lo que les importa”⁵⁹. Actualmente se ha producido un cambio al interior de la compañía propietaria de esta red social, si bien la aplicación continúa llamándose Facebook, sus dueños ahora son META.⁶⁰

Los usuarios que acceden a esta red social en línea, la utilizan para distintos objetivos, algunos le dan un sentido de información actualizada permanente, otros con el objetivo de socializar, encontrar o buscar amigos, publicar fotografías, compartir estados emocionales, extender la red de contactos profesionales, etc.

Desde ya hacemos presente que para poder analizar el uso de la huella digital del usuario de internet en esta red social nos debemos remitir a la política de datos y condiciones de servicio publicada por Facebook en su página oficial⁶¹ ya que, a diferencia de Twitter, se mueve en un ambiente distinto denominado *semicerrado*. La importancia de lo recién señalado radica principalmente que en Facebook los usuarios adquieren una responsabilidad mayor con el tratamiento de su huella digital, considerando que será decisión suya el publicar diferentes tipos de contenidos, encontrándose al tanto de aquellos, que, según la política de términos y condiciones de Facebook, serán puestos a disposición tanto por la empresa en sí misma, como por empresas publicitarias, entre

⁵⁹ Casado, op.cit. p. 32.

⁶⁰ Meta Platforms, Inc., cuyo nombre comercial es Meta, es un conglomerado estadounidense de redes sociales. Actualmente son dueños además de otras redes sociales como Instagram, Whatsapp, entre otras, y si bien se ha mantenido el funcionamiento de las mismas de manera separada, tal adquisición responde a la visión de uno de sus dueños y fundadores, Mark Zuckerberg, denominada *Metaverso*, el cual en palabras del mismo Zuckerberg se refiere a una realidad virtual que en un futuro servirá para conectar a las personas de todo el mundo en entornos tridimensionales donde vivir experiencias compartidas.

⁶¹ Facebook. (22 de octubre de 2020). *Condiciones de Servicio*. <https://es-es.facebook.com/legal/terms>

otras. Acá los límites son más difusos, y por ello, es fácil caer en acciones arbitrarias contra los usuarios y muchas veces actos ilegales, que contravienen incluso los principios básicos de toda relación contractual.

Facebook, como empresa y red social es un conglomerado, posee un equipo multidisciplinario que no solo maneja la empresa frente a otras entidades (públicas y privadas) sino que también frente a los miles de millones de usuarios que posee.

Lo anterior queda en evidencia con la redacción de las cláusulas detrás de su política de datos y condiciones de servicio, que cualquiera podría llamar una *joya legal*, ya que por cada dos beneficios que la empresa significa al usuario de internet, éste la exonera de responsabilidad en, al menos, tres faltas (o posibles delitos) que se pueden cometer por el uso y tratamiento de la información que manipulan. Y todo ello escudado bajo el aparente consentimiento del usuario manifestado al pinchar el recuadro de *Acepto términos y condiciones de servicio*.

A continuación, analizaremos aquellos aspectos de estos términos y condiciones de servicio publicados por Facebook que nos parecen más importantes y que evidencian la complejidad del uso y tratamiento de la información de los usuarios en ambientes semicerrados.

Exoneración de responsabilidad por medio de un contrato de adhesión y política de privacidad.

Si bien META, la idea del metaverso y la nueva realidad virtual que plantean ha logrado de cierta manera desviar el foco de los problemas que aquejan a Facebook, no significa que se han solucionado. Un claro ejemplo de ello, dice relación con el caso de filtración de documentos por parte de una ex empleada de la red social que expone y evidencia la incapacidad de reacción o la lentitud de la empresa, frente a situaciones en que le corresponde actuar como moderadora (según su propia política de términos y condiciones de uso) y no lo hace o lo hace deficientemente por encontrarse atada de manos ante la impunidad y el ya conocido, pero mal utilizado, derecho al anonimato. De esta forma, aquellos aspectos que no fueron abordados en el contrato de adhesión se transforman en

terreno de nadie y muchas veces, sirven de justificación, para cometer actos ilícitos por ser una zona gris y que no se ha visto debidamente regulada por las leyes.

Sin ir más lejos, Facebook indica que no se hace responsable

“de las acciones, el contenido, la información o los datos de terceros y por la presente nos dispensas a nosotros, nuestros directivos, empleados y agentes de cualquier demanda o daños, conocidos o desconocidos, derivados de o de algún modo relacionados con cualquier demanda que tengas interpuesta contra tales terceros.”⁶²

Tal como analizamos en el apartado de las cláusulas de exención y limitación de responsabilidad, este sitio web, establece un estándar de irresponsabilidad (y no de responsabilidad como debería ser) en donde transforma al usuario digital en el principal responsable de sus acciones, pero además lo vuelve responsable ante el debido funcionamiento del sitio web y para con terceros. Incluso señala que “no será responsable ante los daños conocidos o desconocidos” ⁶³, dicha exención de responsabilidad tiene alcances importantes, pues no solo se refiere al sitio web, sino que además comprende a sus directivos, empleados y agentes.

En esta suscripción en bloque que realiza el usuario de Facebook, también adhiere a la política de privacidad de la empresa y a sus principios, “sin derecho a réplica u observaciones”⁶⁴ en donde pareciera ser que el usuario no logra visualizar realmente a qué está renunciando, tampoco sería sencillo culparlo de aquello toda vez que la empresa utiliza frases captadoras de seguridad y confianza como las que siguen:

- “Te damos control sobre tu privacidad.
- Ayudamos a las personas a comprender cómo se utilizan sus datos.
- Incluimos opciones de privacidad en nuestros productos desde el comienzo.

⁶² Facebook, Loc.cit.

⁶³ Facebook, Loc. cit.

⁶⁴ Es importante hacer la diferenciación entre el derecho a réplica que tiene un contratante versus la posibilidad que otorga la empresa para realizar observaciones sobre el funcionamiento del servicio. La primera se refiere derechamente a la manifestación de voluntad de un contratante para formular modificaciones a ciertas cláusulas de un contrato con las cuales no se siente conforme, y la segunda, al simple hecho de comentar sobre la calidad de un servicio, que finalmente sirve de feedback a la empresa y no al usuario.

- Tu información es tuya y puedes eliminarla.
- Somos responsables⁶⁵.

Estos principios de privacidad y responsabilidad a los cuales hace propaganda Facebook en su página oficial se contraponen directamente, en primer lugar, con la letra chica de su cláusula de limitación de responsabilidad, en donde menciona:

“no tenemos control ni influencia sobre lo que las personas hacen o dicen. Asimismo, no somos responsables de sus comportamientos o acciones, ya sea dentro o fuera de internet, ni del contenido que comparten, incluido aquel que pueda resultar ofensivo, inapropiado, obsceno, ilegal o cuestionable.”⁶⁶

Esto quiere decir, que Facebook en vez de establecer una cláusula de responsabilidad más bien plantea una política de exención de la misma.

Y, en segundo lugar, al imponer al usuario la presión de que para poder acceder a sus productos debe concederle permisos sobre determinados contenidos que este sube a su cuenta, por ejemplo: “Permiso para usar el contenido que creas y compartes, permiso para usar tu nombre, tu foto de perfil e información sobre las acciones que realizas en anuncios y contenido patrocinado y permiso para actualizar el software que usas o descargas”⁶⁷. En realidad lo que ocurre con este tipo de aceptación forzada es que se obliga al usuario a *aceptar* en bloque términos y políticas de uso a cambio de acceder a productos de manera gratuita, escondiendo con ello un negocio de tratamiento de datos personales con los cuales, finalmente, la empresa lucra y que es fuertemente criticado desde el punto de vista de la teoría liberal⁶⁸ (justamente en aquello que se refiere a la propiedad de la información personal de los usuarios de la web y su posibilidad de ser comercializada por ellos mismos).

⁶⁵ Facebook. Loc.cit.

⁶⁶ Facebook. Loc.cit.

⁶⁷ Facebook, Loc. cit.

⁶⁸ Revisar capítulo I. De los diversos tipos de información. Subcapítulo II Teorías de la propiedad de la información: Teoría restrictiva y Teoría Liberal.

Uso de datos personales y tratamiento de la información de los usuarios en Facebook.

En la política de términos y condiciones de uso se señala claramente que “A fin de proporcionarte los Productos de Facebook, debemos tratar información sobre ti. El tipo de información que recopilamos depende de la forma en la que usas nuestros Productos”⁶⁹. En este sentido, Facebook indica el tipo de información que recopila, sus fuentes y en qué consiste su tratamiento dividiéndola en tres grupos, a saber:

1. “Lo que tú y otras personas hacen y proporcionan: Información y contenido que nos proporcionas, las redes y conexiones, tu uso de nuestros Productos, información sobre transacciones realizadas en nuestros Productos y la actividad de otros usuarios y la información que proporcionan sobre ti.
2. Información de los dispositivos: Como se describe a continuación, recopilamos información de las computadoras, los teléfonos, los televisores conectados y otros dispositivos conectados a la web que usas y que se integran con nuestros Productos, y combinamos esta información entre los diferentes dispositivos que empleas.
3. Información de los socios: Los anunciantes, los desarrolladores de apps y los editores pueden enviarnos información por medio de las herramientas empresariales de Facebook que usan, incluidos nuestros plugins sociales (como el botón "Me gusta"), el inicio de sesión con Facebook, nuestras API y SDK, o el píxel de Facebook. Estos socios nos brindan información sobre las actividades que realizas fuera de Facebook, incluidos datos sobre el dispositivo que utilizas, los sitios web que visitas, las compras que haces, los anuncios que ves y la manera en la que usas sus servicios, ya sea que tengas o no una cuenta de Facebook o hayas iniciado sesión en ella”⁷⁰.

⁶⁹ Navas, op.cit. pp 1-2.

⁷⁰ Facebook, Loc. cit.

El negocio publicitario de los datos personales de los usuarios en Facebook.

“La información y la economía se encuentran relacionadas en distintos e importantes aspectos, es así como la información constituye un factor relevante al momento de establecer supuestos en un determinado modelo económico, como sucede, por ejemplo, en la existencia de mercados de competencia perfecta, ya que si no hubiese información perfecta entre los agentes que participan en el mercado no se lograría un equilibrio competitivo y eficiente. De otra parte, la posesión de información por sólo uno de los agentes en una determinada transacción, es tratada en la ciencia económica como una falla de mercado, la denominada asimetría de información. Dentro de las múltiples relaciones existentes entre los conceptos mencionados, de las cuales sólo se han expuesto aquí algunas, centraremos nuestro estudio en este primer acápite en la información como bien económico, es decir, como un objeto que posee valor en el mercado y que, por lo tanto, es transado.”⁷¹

Como hemos mencionado anteriormente, las empresas publicitarias son una fuente trascendental de ingresos para estos sitios web, obviamente Facebook no es la excepción, por ello ha establecido en sus términos de uso un apartado que trata directamente a la publicidad, la cual si bien no es detallada ni extensa, es importante ya que establece un criterio específico sobre su funcionamiento y los aspectos publicitarios a los cuales se ven expuestos los usuarios de este sitio web al suscribir el contrato de adhesión. Se señala que “en lugar de pagar por usar Facebook y el resto de los productos y servicios que ofrecemos, al usar los Productos de Facebook que se incluyen en estas Condiciones, aceptas que podamos mostrarte anuncios de las empresas y organizaciones que nos pagan por promocionarse dentro y fuera de los Productos de las empresas de Facebook. Usamos tus datos personales, como la información sobre tu actividad y tus intereses, para mostrarte aquella publicidad que pueda resultarte más relevante”⁷²

A la luz de lo antes expuesto, consideramos que Facebook hace un abuso en su política de términos y condiciones de uso, en donde explícitamente limita su responsabilidad, obliga al usuario a adherirse a sus principios de privacidad a cambio del uso de sus productos y le entrega una apariencia de seguridad y confianza en la administración y

⁷¹ Jervis, op.cit. p.21.

⁷² Facebook, Loc. cit.

difusión de los datos personales que maneja, encubriendo con ello que existen zonas grises que carecen de regulación y ante las cuales no puede realizar el papel moderador al cual se compromete. Sería contraproducente olvidar que la información que suministran las empresas de sus políticas de privacidad, tienen un redacción compleja por no decir, ininteligible para un usuario promedio, donde además complejizan más el asunto haciendo pasar al usuario de un link a otro, con el objeto deliberado de que nunca alcance un conocimiento cabal y completo.

CAPÍTULO III. PROCESAMIENTO DE LA INFORMACIÓN EN LA WEB: USO Y TRATAMIENTO.

I. Conceptos clave.

Privacidad digital.

Para abordar este concepto se requiere, en primer término, remitirnos al estudio de la Psicología, la que al representar al ser humano en su aspecto social nos deriva hacia el campo de la psicología ambiental⁷³. En tales términos, “la privacidad puede referirse a la idea de estar solo, alejado físicamente de otras personas o de algunas -ya que el elemento de referencia puede ser la persona o el grupo. Por otra parte, se considera una situación de privacidad cuando la persona o el grupo puede regular efectivamente la información que ofrece ante los otros”⁷⁴ y en un sentido dogmático, en cita a Irwin Altman, la identifica como: “el control selectivo del acceso a uno mismo o al grupo al que uno pertenece”⁷⁵. Destacando de aquello la subsecuente y estrecha relación de la privacidad en un aspecto dual referido al control, por parte del agente, tanto de su actividad interpersonal con el entorno y otros individuos, así como en relación a la selección de la información que decide compartir y tomar para sí, proveniente del exterior. De allí que se distingan manifestaciones o formas de la privacidad: Si nos referimos al control de la interacción: Soledad y aislamiento. En cuanto al control selectivo de la información: Anonimato y reserva. Y en un tercer aspecto, en referencia al individuo en su contexto grupal: La intimidad⁷⁶. Dentro de tal, una de las funciones principales de la privacidad se orienta hacia la identidad personal y sus subfunciones: Autoidentidad, autoevaluación y autonomía personal⁷⁷.

En tal orden de ideas podemos comprender de manera más acabada a la privacidad digital como el “derecho de los usuarios a proteger sus datos en la red y decidir qué

⁷³ Universitat de Barcelona. Departamento de Psicología Social y Psicología Cuantitativa. *Introducción*. http://www.ub.edu/psicologia_ambiental/introduccion

⁷⁴ Op. cit.. *Introducción al concepto de privacidad*. http://www.ub.edu/psicologia_ambiental/unidad-3-tema-5

⁷⁵ Op. cit.. *Definición de privacidad*. http://www.ub.edu/psicologia_ambiental/unidad-3-tema-5-1

⁷⁶ Op. cit.. *Las formas de la privacidad*. http://www.ub.edu/psicologia_ambiental/unidad-3-tema-5-2

⁷⁷ Op. cit.. *Las funciones de la privacidad*. http://www.ub.edu/psicologia_ambiental/unidad-3-tema-5-3

información está visible para el resto”⁷⁸. Donde el contexto de desenvolvimiento del sujeto pasa a ser un intangible, cual es internet, una herramienta informática de transmisión de datos en formato digital de nivel global al alcance de cualquier individuo o grupo de agentes, quienes actúan siendo tanto transmisores como receptores de información de diversa índole, para quienes antaño existía una barrera de entrada de nivel económico importante, lo cual dificultaba su acceso y alcance al grueso poblacional, pero que en la actualidad representa un nivel de tráfico masivo, de fácil acceso, que importa una conectividad total de carácter global, llegando a tal grado de expansión y relevancia que se han acuñado términos tales como el Internet de las Cosas (“IoT” por sus siglas en inglés) para incluir en esta discusión a todo aquello orientado hacia el intercambio de información digital con objetos de uso cotidiano como electrodomésticos, relojes o mobiliarios del hogar. Aparatos que a su vez recogen información privada del usuario pudiendo “estar implicados en el tratamiento, generación y recogida de los datos (...)”. Consecuentemente, la mayor parte de ellas estarán interesadas en cierto grado en ser los propietarios de la totalidad o parte de la información y por ello ser titulares del derecho de usar, mantener, transmitir o vender a –i.e. “monetizar”- los datos a terceros interesados”⁷⁹, todo lo cual nos informa de manera concreta en cómo el devenir de la expansión, crecimiento y multiplicidad de formas en que va evolucionando la sociedad, en estrecha interrelación con la tecnología, nos permite observar cuán relevante se torna el debate y el cuestionamiento acerca de la privacidad de los datos, toda vez que las decisiones tomadas en relación revisten un mayor grado de relevancia y trascendencia.

Autodeterminación informática.

Íntimamente ligado a al concepto de autodeterminación informática encontramos su origen, en concepto de Cerda⁸⁰, en el derecho a la intimidad y el “privacy” americano, indicando que tal derecho obtuvo reconocimiento jurídico internacional recién con la Declaración Universal de Derechos Humanos de 1948, la que en su artículo 12 prescribe que “nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación”, teniendo derecho a

⁷⁸Tablado, F., Grupo Atico 34 (8 de Enero de 2020) *Guía sobre la privacidad digital*. https://protecciondatos-lopdp.com/empresas/privacidad-digital/#Que_es_la_privacidad_digital

⁷⁹ Osborne Clarke. *Internet de las cosas y propiedad sobre la información*. <https://www.osborneclarke.com/es/insights/internet-de-la-cosas-y-propiedad-sobre-la-informacion>

⁸⁰ Cerda, A.. Op. cit.. p.4

ser protegido por la ley quien fuere víctima de dichos ataques⁸¹. Y luego, a partir de este punto es que se ha ido configurando el panorama normativo moderno, sobretodo en atención a que “las estructuras normativas surgidas en la modernidad y en la etapa en la codificación no han podido sustraerse a los efectos de la creciente aplicación de las nuevas tecnologías que caracteriza a la “sociedad de la información”⁸², lo cual, con el devenir de la era moderna y “la intromisión de la informática y las telecomunicaciones en el quehacer cotidiano ha obligado a una reformulación conceptual del derecho a la intimidad, en términos de ser concebido como “el derecho del individuo a decidir por sí mismo en qué medida quiere compartir con otros sus pensamientos y sentimientos, así como los hechos de su vida personal”⁸³.

Tipos de datos.

Un dato, según precisa Cerda⁸⁴, es “una unidad básica de información”. A la luz de la normativa chilena vigente, la Ley 19.628 en su artículo 2° conceptualiza expresamente cuatro tipos de datos:

- **Datos de carácter personal o datos personales:** los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.
- **Datos sensibles:** aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.
- **Dato caduco:** el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.

⁸¹ Art. 12. Naciones Unidas (1948). *Declaración Universal de Derechos Humanos*. <https://www.un.org/es/about-us/universal-declaration-of-human-rights>

⁸² Cerda, A., Op. cit. p.6

⁸³ Op. cit. p.7

⁸⁴ Op. cit. p.16

- **Dato estadístico:** el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.

Suma la ley a lo anterior conceptos tales como:

- **Almacenamiento de datos:** la conservación o custodia de datos en un registro o banco de datos.
- **Registro o banco de datos:** el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.
- **Tratamiento de datos:** cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

II. El ámbito de lo permitido conforme a la normativa vigente.

Si bien, en un primer estadio normativo, “la autodeterminación informativa o libertad informática carece de reconocimiento en tratados internacionales sobre derechos humanos, pues la mayor parte de ellos fueron aprobados con anterioridad a que se suscitara problemas jurídicos en relación con el tratamiento automatizado de datos personales”⁸⁵, organizaciones tales como Naciones Unidas o la Unión Europea avanzan sobre la materia, emitiendo directrices en el caso de la primera⁸⁶ y en el caso de la segunda, con la Carta de los Derechos Fundamentales de la Unión Europea⁸⁷, reconociendo como un derecho en su artículo 11° a la libertad de expresión y de

⁸⁵ Cerda, A., Op.cit. p.10

⁸⁶ Asamblea General de la Naciones Unidas. *Principios rectores para la reglamentación de los ficheros computarizados de datos personales* [archivo pdf]. Resolución 45/95. 14 de Diciembre de 1990. <http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf>

⁸⁷ Carta de los derechos fundamentales de la Unión Europea (18 de Diciembre de 2000) [archivo pdf]. p.11. https://www.europarl.europa.eu/charter/pdf/text_es.pdf

información, y consagrando en su artículo 8° la protección de datos de carácter personal⁸⁸ de cuya lectura se desprende el establecimiento de una base de amparo legal que asiste a todas las personas en conjunto con directrices ético-normativas en relación al tratamiento de sus datos personales, sobre la base del consentimiento del titular o la ley.

Progresivamente estos conceptos derivados de la vida privada adquieren mayor visibilidad, “desde un criterio económico, centrado principalmente en la transacción internacional de datos (datos transfronterizos), lo que dice estrecha relación con el carácter económico de los organismos internacionales que se pronuncian al respecto”⁸⁹. Siendo así y actuando como agente internacional de cambio, la OCDE trata la protección de datos personales de manera innovadora desarrollando “estas directrices en base a los tres principios que agrupan a los estados que conforman esta institución: la democracia pluralista, el respeto de los derechos humanos y las economías de mercado abiertas”⁹⁰, siendo concerniente su aplicación tanto en el ámbito público como privado, destacando “un catálogo de principios de aplicación nacional, donde destacan el principio de consentimiento, de calidad, finalidad, seguridad y responsabilidad. (...) Igualmente genera principios para el flujo transfronterizo de datos, donde destaca la libre circulación de estos”⁹¹.

Modernamente, el desarrollo legislativo avanza hacia un concepto no sólo de índole económica, sino que se agrega un reconocimiento a los aspectos sociales y culturales involucrados en la materia, donde se busca “proteger el tratamiento de datos personales ante los peligros que genera el vertiginoso avance de las tecnologías de la información”⁹².

Destacan dentro de este grupo de normativas, los Estándares Internacionales conocidos como la “Resolución de Madrid”⁹³, los que reafirman “la factibilidad de avanzar hacia un documento internacionalmente vinculante, que contribuya a una mayor protección de los

⁸⁸ Op. cit. p.10

⁸⁹ Cámara de Diputados de Chile. *Evaluación de la Ley N° 19.628* [archivo pdf]. p.17. http://www.evaluaciondelaley.cl/wp-content/uploads/2019/07/informe_final_ley_19628_con_portada.pdf

⁹⁰ Op. cit. p.18

⁹¹ Loc.cit.

⁹² Op.cit. p.19

⁹³ Resolución de Madrid (2010). *Estándares Internacionales sobre Protección de Datos Personales y Privacidad* [archivo pdf]. Agencia Española de Protección de Datos. https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf

derechos y libertades individuales en un mundo globalizado, y por ello, caracterizado por las transferencias internacionales de información”⁹⁴.

En este punto, de suma importancia resulta detenernos en el análisis de los conceptos involucrados, en cuanto representa gran trascendencia para las futuras legislaciones locales.

A.- Resolución de Madrid⁹⁵

“La labor conjunta de los garantes de la privacidad de casi cincuenta países, bajo coordinación de la Agencia Española de Protección de Datos, ha desembocado en un texto que trata de plasmar los múltiples enfoques que admite la protección de este derecho, integrando legislaciones de los cinco continentes. Su carácter consensuado aporta dos valores añadidos esencialmente novedosos: de un lado, enfatiza la vocación universal de los principios y garantías que configuran este derecho; del otro, reafirma la factibilidad de avanzar hacia un documento internacionalmente vinculante, que contribuya a una mayor protección de los derechos y libertades individuales en un mundo globalizado, y por ello, caracterizado por las transferencias internacionales de información.”

En tales términos reza la presentación de la Resolución de Madrid, encabezada por don Artemi Rallo Lombarte, director de la Agencia Española de Protección de Datos, quien expresa como derrotero el que “las autoridades de supervisión y control de la privacidad asumimos la exigente tarea de difusión y promoción desde nuestro firme compromiso de garantizar a nuestros ciudadanos una mejor protección de la privacidad y de los datos de carácter personal

Así, la resolución de la Comisión, en su 2º numerando, identifica y define conceptos clave tales como: Datos de carácter personal, tratamiento, interesado, persona responsable y prestador de servicios de tratamiento. El ámbito de aplicación considera tanto al sector público como privado, estableciéndose como base regulatoria, permitiendo las transferencias internacionales de datos de carácter personal siempre que se sujeten al

⁹⁴ Cerda, A., Op. cit.. p.19

⁹⁵ Resolución de Madrid. Op. cit. p.3

procedimiento indicado en el mismo cuerpo normativo⁹⁶, de lo que se observa cómo desde su inicio, se comprende no sólo la diferenciación a realizarse según el tipo de dato que se trata así como también, en relación a la privacidad de los datos de carácter personal -objeto principal de materia del documento en comento- sino que a su vez se entiende que no corresponde a un ámbito únicamente de carácter e interés local, lo que deja en evidencia el alto grado de trascendencia de la materia, denotando que la intercomunicación de datos personales a nivel extraterritorial es un hecho y que por tanto la vía idónea es la regulación de su tratamiento.

En cuanto límites de los alcances de la regulación, se deja constancia expresa que los Estados pueden fijar límites propios en cuanto sean a consecuencia de un interés general “para preservar la seguridad nacional, la seguridad pública, la protección de la salud pública, o la protección de los derechos y las libertades de los demás Tales limitaciones deberán estar expresamente previstas por el derecho interno, de tal modo que se establezcan sus límites y se prevean las garantías adecuadas para preservar los derechos de los interesados”⁹⁷.

En paralelo, establece una serie de principios básicos que deben primar en el tratamiento y procesamiento de los datos, como son el de lealtad y legalidad, de finalidad, proporcionalidad, calidad, transparencia y responsabilidad⁹⁸. Además insta de manera específica la categoría de dato personal sensible, entre los que incluye a aquellos datos “que afecten la esfera más íntima del interesado”⁹⁹, detallando posteriormente que se consideran a “aquellos datos de carácter personal que puedan revelar aspectos como el origen racial o étnico, las opiniones políticas o las convicciones religiosas o filosóficas; así como los datos relativos a la salud o a la sexualidad”¹⁰⁰, lo que deja en evidencia la estrecha relación que hay entre esta categoría específica de dato privado con el ámbito y derecho de las personas a su intimidad, en una heterogénea gama de aspectos que, en estados democráticos, se le asocian social y culturalmente a todo cuanto involucra la privacidad del individuo, pero que al ser expuesta y obtener reconocimiento expreso,

⁹⁶ Artículo 4 Resolución de Madrid: “Las disposiciones del presente Documento constituirán base apropiada para permitir las transferencias internacionales de datos de carácter personal, cuando éstas se realicen según lo indicado en el apartado 15 del presente Documento”.

⁹⁷ Op. cit. Art. 5.

⁹⁸ Op. cit. Arts. 6-11

⁹⁹ Op. cit. Art. 13 N°1 letra a)

¹⁰⁰ Op. cit. Art. 13 N°2

brinda un marco jurídico y de control al momento de reclamar una posible infracción en su contra, cuestión que implicaría una vulneración en términos vinculares contractuales ya que se le impone a la persona responsable del tratamiento de datos una relación de tal carácter con el sujeto, derivado del reconocimiento expreso que realiza la norma en su artículo 15° letra b) del deber de configurar el vínculo “a través de un contrato u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido, y que establezca el compromiso del prestador de servicios de tratamiento de cumplir con estas garantías y de asegurar que los datos de carácter personal sean tratados siguiendo las instrucciones de la persona responsable”¹⁰¹.

De esta manera, se hace patente la dualidad en el tratamiento o procesamiento de los datos personales, reconociendo y garantizando por una parte, la titularidad de cada individuo respecto de su información privada, haciendo uso de ella conforme lo estime pertinente para sus propios fines o intereses, pudiendo a su vez conceder derechos de representación sobre los mismos, además de autorización directa a un tercero quien, por otra, será el responsable del tratamiento de esos datos privados, sin perder el primero, al ser derechos personalísimos, su titularidad o dominio sobre su bien jurídico en favor de ningún otro, con lo cual se le reconoce una serie de garantías que le amparan en el legítimo ejercicio del resguardo de la privacidad e intimidad a que tiene derecho. Así, se declama entre los artículos 16 a 18 que el sujeto detenta en cuanto titular, derechos de acceso, de oposición y de rectificación y cancelación en lo que respecta al tratamiento de sus datos. Con esto, se identifica en un aspecto la facultad de uso arbitrario que le ampara al sujeto titular respecto de sus datos personales y por otro, los deberes y responsabilidad que le asisten al responsable, sea persona individual o sea prestador de servicios de tratamiento de dichos datos; todo aquello encuadrado dentro de un marco normativo de carácter especial y específico, atendida la naturaleza sensible del bien jurídico custodiado.

En lo que al tratamiento de datos refiere, la Resolución contempla una serie de deberes de cuidado y líneas guía, sobretudo en atención a los derechos de los usuarios. Tal es así que, para representar al sujeto, el prestador de servicios de tratamiento ha de constituirse como tal sujetándose a las reglas de la legislación en particular, debiendo ceñir la relación

¹⁰¹ Op. cit. Art. 14

jurídica a un iter contractual que acredite la existencia, alcance y contenido de la misma, asegurando que los datos sean tratados de la forma prevista por la legislación.

En particular, se le reconocen al interesado los derechos de acceso, rectificación y cancelación y de oposición, y en el ámbito de la seguridad, los derechos de oposición y confidencialidad¹⁰². Enseguida, la norma reconoce al responsable de los daños y/o perjuicios, el deber de reparación, tanto material como moral.

Es menester señalar que, a modo de epígrafe -indica la Conferencia que- la Resolución adopta como derrotero “la urgente necesidad de proteger la privacidad en un mundo sin fronteras, y de alcanzar una propuesta conjunta para el establecimiento de estándares internacionales sobre privacidad y protección de datos personales” manera tal que las legislaciones en la materia adopten un “(...) enfoque más uniforme a nivel internacional:

- a. De manera leal, lícita, y proporcionada en relación con finalidades determinadas, explícitas y legítimas.
- b. Sobre la base de políticas transparentes, informando adecuadamente a los interesados y sin ninguna discriminación arbitraria en su contra.
- c. Garantizando la exactitud, la confidencialidad y la seguridad de los datos, así como la legitimidad del tratamiento, y los derechos de los afectados a acceder, rectificar y cancelar los datos, así como a oponerse a un determinado tratamiento.
- d. Aplicando el principio de responsabilidad, incluyendo la responsabilidad por daños, incluso si las operaciones de tratamiento se llevan a cabo por prestadores de servicios que actúen por cuenta del responsable.
- e. Ofreciendo garantías más adecuadas cuando los datos son sensibles.
- f. Garantizando que los datos personales transferidos internacionalmente se benefician del nivel de protección previsto en el mencionado conjunto de estándares.

¹⁰² Op. cit. Arts. 16 - 21

g. Sometiendo el tratamiento a la vigilancia de autoridades de supervisión, independientes e imparciales, con poderes y recursos adecuados, y sometidas a un deber de cooperación entre sí.

h. En un marco nuevo y moderno de medidas proactivas, orientadas en particular a prevenir y detectar infracciones y basadas en la designación de oficiales de privacidad, así como en auditorías eficaces y en evaluaciones de impacto de privacidad.”

En cuanto normativa comparada, fuera de España, destacan la Unión Europea (UE) y en Latinoamérica, la legislación de Uruguay.

B.- Marco Normativo Ley 19.628

Históricamente, nuestra legislación chilena carecía de un marco normativo robusto en cuanto protección a la intimidad, privacy o autodeterminación informática, siendo el numerando 4° del artículo 19 de la Constitución, que asegura “[e]l respeto y protección a la vida privada y a la honra de la persona y su familia” la garantía normativa de usual recurrencia para articular una extensión de la misma y buscar así dar protección frente al tratamiento de los datos personales¹⁰³, convirtiéndose el recurso de protección en la vía que mejor cabida daba en consideración a esta precario marco normativo previo a la Ley 19.628 (en adelante, indistintamente, la Ley)

En tal orden de ideas, en el ámbito penal también resultaba escueto e insuficiente la normativa aplicable, ya que consideraba unos cuantos ejemplos específicos según relación laboral o en orden a normativa sanitaria, sin contemplar disposiciones directas y específicas en materia de tratamiento de datos personales.¹⁰⁴

En este escenario normativo es que llega a regir para el año 1999 la Ley 19.628 sobre protección a la vida privada.

¹⁰³ Cerda, A., Op. cit. p.13

¹⁰⁴ Loc.cit.

En cuanto derecho comparado, Cerda describe que “existen dos tendencias respecto de la extensión que debe abrigar una ley relativa al tratamiento de los datos personales: de un lado, quienes estiman del caso la adopción de una ley uniforme aplicable a todo evento en que deba brindarse protección frente al tratamiento; de otros, quienes estiman apropiado adoptar leyes sectoriales, a fin de hacer frente a las peculiaridades que sean demandadas, según la naturaleza de los datos tratados o de la entidad titular del banco de datos¹⁰⁵”. Para el caso de la nuestra, ésta adopta un carácter mixto, esto es una “norma marco” que ha de ir nutriéndose y siendo referencia obligada en cuanto surgimiento y crecimiento de normativa sectorial posterior sobre la materia.

i) Principios que recoge la Ley 19.628

- a) Principio de Libertad
- b) Principio de Licitud y Lealtad
- c) Principio de Información y Consentimiento
- d) Principio de Finalidad
- e) Principio de Calidad de los Datos
- f) Principio de Seguridad
- g) Deber de Secreto

ii) Ámbito de aplicación de la Ley 19.628

Según señala en su artículo 1°, la ley regula el tratamiento de los datos de carácter personal, tanto en ámbito público como privado y particulares, salvo que se trate del tratamiento en el ejercicio de las libertades de emitir opinión e informar, siempre que el mismo se haga de manera concordante a sus principios y prerrogativas y dentro de lo permitido por el propio ordenamiento jurídico.

En lo relativo a la extensión de aplicación de la misma, el ordenamiento se aún en dos posturas clave: “de un lado, quienes estiman del caso la adopción de una ley uniforme aplicable a todo evento en que deba brindarse protección frente al tratamiento; de otros, quienes estiman apropiado adoptar leyes sectoriales, a fin de hacer frente a las

¹⁰⁵ Cerda, A., Op. cit. p.15

peculiaridades que sean demandadas, según la naturaleza de los datos tratados o de la entidad titular del banco de datos”¹⁰⁶.

En nuestro caso particular nacional, el legislador optó por una normativa marco, o como denomina Cerda, una *ley ómnibus*¹⁰⁷ la cual establecida como legislación general, hace posible su aplicación a diversos contextos, lo que se viene a integrar con la legislación posterior en ámbitos sectoriales específicos, puesto que ha de regir como norma fundante, según indica el tenor del artículo primero de la Ley 19.628: “El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar”. Previamente, al referirnos a los conceptos clave de la ley, comprendimos que en lo relativo a esta materia, el legislador indica una visión amplia, lo cual manifiesta la intención de abarcar la mayor cantidad de situaciones posibles, en el entendido que el tratamiento puede realizarse por diversas vías, en distintas situaciones, mediante un sinnúmero de acciones que producto del avance de la tecnología, entiende el legislador es posible no sea capaz de abarcar en el momento de dictación de la misma, lo que puede redundar en una desprotección del individuo, razón por la que al referirse al tratamiento de datos, lo expresa de forma general como “cualquier operación o complejo de operaciones o procedimientos técnicos”¹⁰⁸ así como posterior a brindar un detalle de las distintas maneras en que puede entenderse y realizarse esta operación para el uso de los datos, concluye con “o utilizarlos en cualquier otra forma”, que deja patente esta apertura en cuanto la transversalidad y multiplicidad de situaciones y usos posibles sobre los datos personales, así las cosas, el legislador instaura esta normativa general, dando pie a las normativas sectoriales para establecer el uso regulado en la materia, tanto por instituciones públicas y privadas.

¹⁰⁶ Cerda, A., Loc. cit.

¹⁰⁷ Loc. cit.

¹⁰⁸ art. 2 Ley 19.628 de 1999. *Sobre protección de la vida privada*. Agosto de 1999.

III. El ámbito de lo permitido conforme a la voluntad explícita y tácita

Libertad en el tratamiento de datos en Chile

“La Ley permite el tratamiento de datos personales siempre que se haga de manera concordante con ésta y para finalidades permitidas por el ordenamiento jurídico. Asimismo, consagra el respeto al pleno ejercicio de los derechos fundamentales de los titulares de los datos y a las facultades que la norma les reconoce”¹⁰⁹. Así mandata en su artículo 1° inciso segundo: “Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce.”

Los anterior nos comanda hacia la libertad general que existe para el legislador respecto del tratamiento de los datos personales, hecho posible de realizar por toda persona, pero que sin embargo ha de sujetarse a los propios límites que se establecen, esto es, que debe realizarse de forma concordante al ordenamiento jurídico y principios de la normativa, sus fines deben ser autorizados por el propio ordenamiento, siempre con miras al respeto del pleno ejercicio de los derechos fundamentales de los titulares y sus facultades reconocidas por la propia ley.

Lo anterior se refuerza en relación al principio de licitud, que vemos plasmado en el artículo 4° de la ley: “El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.”

¹⁰⁹ Cámara de Diputados. Op. cit. p. 34

El consentimiento

Continúa el mismo artículo 4°: “La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público. La autorización debe constar por escrito. La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito.”

La intención legislativa es entonces, establecer el principio de información, esto es que el titular de los datos tenga conocimiento de la recolección de sus datos, los fines o propósitos de aquello y la posibilidad de ser éstos comunicados al público. Puesto que para ser posible el consentimiento, requiere el titular el conocimiento previo de la situación sobre la cual debe manifestar su consentimiento, el que es requerido además por la normativa para así continuar en el resguardo de la tutela de los derechos y garantías fundamentales protegidos por el ordenamiento. En este orden de ideas, se manifiesta que el consentimiento por parte del titular ha de ser “previo, libre e informado”¹¹⁰ así como también puede ser revocado, lo cual nos informa que el consentimiento no ha de ser perpetuo, sino temporal, hecho que no tendrá efectos retroactivos, por cuanto será posible el tratamiento de los datos brindados hasta el momento en que el mismo titular revoque su autorización, sin expresar causa, lo que no hace perder legitimidad al uso anterior ni tampoco confiere una traba para su titular.

Continúa además, con las excepciones en cuanto al consentimiento por parte del titular:

“No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios. Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos”. Para la

¹¹⁰ Cámara de Diputados. Op. cit. p. 31

ley, fuente de libre acceso al público son “los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes”¹¹¹.

En este sentido, entendemos que no se requiere la autorización expresa por el titular en cuanto tres excepciones: la fuente sea de libre acceso al público, el tratamiento sea realizado por personas jurídicas de derecho privado en cuanto su uso exclusivo y con los fines que la misma indica, y en cuanto a los organismos públicos, sólo estará exceptuada la autorización del titular en cuanto se refiera a materias propias de su competencia y con sujeción a la reglas de la normativa del tratamiento de datos personales¹¹².

En relación al consentimiento encontramos también el principio de finalidad y el de calidad de los datos, los cuales versan sobre los “aspectos que deben ser informados al momento de obtener el consentimiento”¹¹³ y que en su artículo noveno detalla: “Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público. En todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos.” Dando cuenta de dos ideas: “por un lado, que la información que proporcionan los datos debe representar fielmente la realidad que predicen; y, por otro lado, que ellos deben ser pertinentes, adecuados y no excesivo respecto del ámbito y objetivo para los cuales fueron recogidos”¹¹⁴.

En cuanto a los datos sensibles, la ley detalla de manera no taxativa en su artículo segundo letra g) como: “aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual” . Acá el legislador invierte la prerrogativa, estableciendo la prohibición de libertad de tratamiento de modo general¹¹⁵, exceptuándose aquellos casos autorizados expresamente por la ley, lo cual resulta del todo relevante y crucial para el análisis

¹¹¹ art. 2 letra i). Ley 19.628 de 1999. Op. cit.

¹¹² art. 20. Ley 19.628 de 1999. Op. cit

¹¹³ Cámara de Diputados. Op. cit. p. 31

¹¹⁴ Cerda, A., p.24

¹¹⁵ Artículo 10 Ley 19.628 de 1999. *Sobre protección de la vida privada*: “No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares”

posterior que deberemos realizar. Así, tales excepciones versan en cuanto la ley autorice tal actividad, exista consentimiento expreso por parte del titular de los datos o cuando éstos sean necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

Finalmente, podemos concluir que para un tratamiento adecuado de los datos personales, conforme a Derecho, hemos de realizar el siguiente proceso evaluativo: 1) Si la Ley 19.628 lo autoriza sin necesidad de consentimiento expreso: Deberá corresponder a una fuente de acceso público, el tratamiento se realizará por personas jurídicas privadas o públicas en el ámbito de su competencia y actividad, y si se trata de datos sensibles ha de ser en cuanto a beneficios de salud que correspondan a sus titulares. 2) Si requiere consentimiento: Ha de ser expreso, informado y siempre con carácter revocable. 3) Otras disposiciones legales lo autorizan: como normativas sectoriales o estatutos especiales, por ejemplo, la Ley General de Bancos o la del Registro Civil e Identificación.

Derechos del titular de datos personales.

Por medio de la ley 21.096 de 2018, se consagra el derecho a protección de los datos personales a nivel constitucional, modificándose el artículo 19, numeral 4° de la Carta Fundamental, resguardando “el respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley”. De esta manera y en concordancia con todo lo anteriormente analizado, podemos inferir que siendo la persona natural el titular de sus datos personales, haciendo la ley eco de aquello y elevando a un carácter de resguardo y seguridad estatutaria especial en cuanto al tratamiento y uso de los mismos, con particular atención a los denominados datos sensibles, se puede entrever que a disposición del titular no sólo quedarían los mecanismos de control que la propia ley integra, sino que todo aquel mecanismo que obre en pos de resguardar las garantías fundamentales, pese a que la ley no señale que entre el titular y sus datos haya un derecho de propiedad¹¹⁶, lo que no deja exento el derecho a

¹¹⁶ Cerda, A.,. Op. cit. p.18

la privacidad y el derecho del titular a la protección de tales datos, en atención a ser víctimas de un tratamiento ilegítimo de sus datos personales¹¹⁷.

En cuanto a los mecanismos integrados por la Ley 19.628, ésta reconoce derechos en favor del titular de los derechos personales “a fin de conferirle efectivo poder de control sobre la recopilación, acopio, procesamiento, uso y transmisión de aquellos”¹¹⁸:

1. Derecho de información o acceso
2. Derecho de rectificación, cancelación y/o bloqueo
3. Derecho a obtener copia
4. Derecho de oposición¹¹⁹

Sobre este último, cabe precisar que nace como correlato al derecho de información del titular, ya que establece a su vez que “[e]l titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión.¹²⁰”

¹¹⁷ Viollier, P., (2017) *El Estado de la protección de datos personales en Chile* [archivo pdf], p.27. <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf>

¹¹⁸ Cerda, A., Op. cit. pp. 27-31

¹¹⁹ Viollier, P., Op. cit. p.26

¹²⁰ Art. 3 inciso final Ley 19.628 de 1999. *Sobre protección de la vida privada*. Agosto 1999

CAPITULO IV. EL PROBLEMA DEL PROCESAMIENTO Y SU USO PARA INCIDIR EN LOS PROCESOS DE DECISIÓN.

I. Problema.

a. Etapas del tratamiento de datos

Previamente definimos lo que debemos entender como tratamiento de datos, esto es una serie de operaciones o procedimientos técnicos que permiten efectuar respecto de los datos personales una serie de acciones que la Ley describe. De este concepto, señala Jervis, se pueden reconocer una serie de “etapas o momentos”¹²¹: a) la etapa de la toma, recolección o recogida de datos personales; b) la etapa del tratamiento de datos propiamente tal, en la cual los datos son tratados --generalmente de forma automatizada--, permitiendo efectuar cruces y relaciones entre los datos; y, c) la etapa de cesión o comunicación de los datos a terceros ajenos a aquél que efectúa el tratamiento en cuestión.

Así, continúa Jervis “[l]o usual es que estas etapas estén todas presentes en el tratamiento de un específico dato personal, pero (...) basta que se realice una sola operación dentro de cualquiera de las etapas para que estemos en presencia de tratamiento de datos personales”¹²²

b. Mecanismo de control

En el capítulo anterior vimos cómo al titular de los datos personales se le reconocen una serie de garantías y derechos, así como principios inspiradores que deben observarse en el tratamiento de los mismos, afianzando hacia un grado constitucional la categoría de tal protección.

Sin embargo y pese a ello, una de las principales críticas hacia la Ley es la ausencia de una autoridad pública de control¹²³, recayendo en primera instancia la

¹²¹ Jervis, P. (2006).La regulación del mercado de datos personales en Chile [Tesis para Magister, Universidad de Chile]. p.51 URI: <http://repositorio.uchile.cl/handle/2250/114258>

¹²² Op.cit., p.52

¹²³Viollier, P., Loc.cit.

responsabilidad de su debido resguardo en los interesados, esto es, en el titular de los datos personales así como en el responsable del registro o banco de datos. En este sentido, la ley no establece un responsable del cumplimiento, debiendo utilizar los afectados los medios jurisdiccionales que dispone la ley, como el mecanismo de la acción constitucional de protección en cuanto se alegare como infracción a las garantías fundamentales.

En el ámbito público, la Ley 20.285 sobre acceso a la información pública otorgó al Consejo para la Transparencia la competencia para velar por debido cumplimiento de la Ley 19.628, lo cual se materializó en el año 2011, mediante una serie de “Recomendaciones sobre Protección de Datos Personales por parte de los órganos de la Administración del Estado”¹²⁴ las cuales tienen por objeto “establecer orientaciones respecto de los criterios jurídicos aplicables por los órganos de la Administración del Estado en el tratamiento de datos de carácter personal que obren en su poder”¹²⁵, las cuales serán aplicables “al tratamiento de datos de carácter personal que efectúen los órganos de la Administración del Estado, entendiéndose por tales los comprendidos en el inciso primero del artículo 2º de la Ley de Transparencia. Las presentes Recomendaciones no serán aplicables a los tratamientos de datos de personas jurídicas, ni al tratamiento de datos de personas fallecidas.”¹²⁶ Así las mismas se dejan en una especie de norma de observancia, más no se entrega un control efectivo y eficiente de cumplimiento del mismo, además de no afectar al ámbito privado, puesto que sólo tiene tal carácter de aplicación para los órganos e instituciones de carácter público.

La persona afectada por la vulneración a la ley puede optar por la utilización del mecanismo jurídico especial contemplado por la Ley 19.628, el cual se ha denominado “acción de habeas data”¹²⁷ la cual “(...) procede en aquellos casos en que el responsable del banco de datos no se pronuncie sobre la solicitud de información, modificación, cancelación o bloqueo en un plazo de dos días hábiles

¹²⁴ Consejo Directivo del Consejo para la Transparencia (31 de agosto de 2011) *Recomendaciones del consejo para la transparencia sobre protección de datos personales por parte de los órganos de la administración del Estado* [archivo pdf]. p.1 <https://www.consejotransparencia.cl/wp-content/uploads/2020/01/RECOMENDACIONES-Para-organismos-del-Estado.pdf>

¹²⁵ Op. cit. p.2

¹²⁶ Loc. cit

¹²⁷ Viollier, P., Op.cit. p.27

o cuando ésta sea denegada¹²⁸. Al efecto, contempla la ley la aplicación de un procedimiento breve y sumario.

c. Transmisión de datos a terceros.

Diversas regulaciones del Derecho comparado, sobretodo aquellas protectoras de datos, hacen referencia a la transferencia de datos personales¹²⁹. Esta comunicación o transferencia puede realizarse tanto de manera internacional como local. En el caso de la primera, la doctrina la denomina como “transmisión transfronteriza de datos personales” y para la segunda, se entiende como tal aquella comunicación de datos que se realiza dentro de los límites de un determinado país. Para el caso de nuestra legislación nacional, la primera situación no se encuentra regulada puesto que se consideró que dicha normativa correspondía a materias de competencia de tratados internacionales¹³⁰. Así, podemos entender que “la transferencia internacional de datos se encuentra permitida en nuestro país, siempre y cuando se cumplan las disposiciones generales establecidas en el texto legal”¹³¹.

Para el caso local, como hemos podido observar, la legislación presenta un silencio no menor en materia de comunicación de datos a terceros, puesto que no exige ni conocimiento ni menos consentimiento respecto a la situación, traduciéndose esto en una pérdida de control por parte del titular respecto de su información, así como la posibilidad de redireccionar la finalidad con la cual se recolectó la misma.

Así, la Ley hace sinónimos a la comunicación con la transmisión¹³²: “La transferencia, se entiende que se produce cuando se comunican datos en forma transfronteriza. La interconexión, se entiende como la acción de conectar entre sí aparatos o sistemas, de forma que entre ellos pueda fluir algo material o inmaterial (en este caso datos personales), finalmente (...) [la] cesión, cuando se entrega a otro la titularidad sobre los bancos o registros de datos personales, ya sea a título

¹²⁸ Viollier, P., Loc. cit.

¹²⁹ Jervis, P., Op. cit. p.91

¹³⁰ Op.cit. p. 93

¹³¹ Loc. cit.

¹³² Loc. cit.

gratuito u oneroso, como por ejemplo, cuando se vende una base de datos”. En conjunto, en el artículo 5° de la Ley, se hace referencia al procedimiento automatizado de transmisión, eximiendo de su aplicación cuando se trate de datos personales accesibles al público en general ni cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes. Tal transmisión automatizada es permitida en la medida que: 1) se cautelen los derechos de los titulares y 2) la transmisión guarde relación con las tareas y finalidades de los organismos participantes. Nada indica la norma respecto a mantener en salvaguarda la finalidad con la cual se recolectaron los datos de manera original, lo que implicaría una consecuencia lógica del principio de finalidad, más que sin embargo no se hace referencia de manera explícita, callando la regulación a su respecto y por ende, provocando un vacío a su respecto.

d. Actores del mercado de datos personales.

Parte de la problemática envuelta en el tratamiento de datos personales obedece al interés económico que generan, así como el mal uso que pueda darse a los mismos. Podemos entender aquello de mejor manera en opinión de Donoso “el objetivo de la Ley debiera ser proteger a las personas respecto del tratamiento de sus datos, sean privados o públicos, porque un tratamiento abusivo de estos datos, aunque sean públicos, puede dar pie a discriminaciones arbitrarias”¹³³

Así, sumado al avance cualitativo y cuantitativo en la utilización de mayor y más eficiente tecnología, se puede observar una desprotección gradual y compleja en el campo de los datos personales y la información personal, puesto que,

“[l]a ley se había dictado en una primera época, donde todo el mundo estaba confundido y pensaba que esto tenía que ver con la privacidad. Hoy en día, el mundo civilizado se dio cuenta, que esta cuestión no tiene que ver con la privacidad. Hay un ámbito de la ley que se refiere a la privacidad, pero un pedacito que se refiere a la privacidad. Existe un gran espacio, donde son datos públicos que si son mal manejados, terminan en abusos o decisiones arbitrarias respecto de las personas”¹³⁴.

¹³³ Cámara de Diputados. Op. cit. p. 35

¹³⁴ Cámara de Diputados. Op. cit. p. 34

Así, el mercado de datos cobra mayor relevancia puesto que contar con datos precisos de información personal acerca del público objetivo se ha vuelto un hito relevante en un proceso que abarca “recolectar, almacenar, procesar, cruzar y comunicar datos personales”¹³⁵

Jervis identifica como actores del mismo¹³⁶: a) como fuentes primarias de información personal, las personas o entidades que entregan al mercado en forma directa datos personales; b) fuentes secundarias de información personal, aquellos que distribuyen la información recibida comunicándola a terceros, y que se encuentran representados por las empresas que se dedican en forma exclusiva a distribuir datos y por aquellos que aun cuando la distribución de datos personales no constituye su giro principal, eventualmente sí distribuyen o comunican datos; c) usuarios finales de los datos personales, aquellos que buscan y adquieren la información personal para uso propio y que pueden ser personas naturales o jurídicas. Todos estos actores pueden figurar dentro de una cadena de transmisión de la información o quizás solo algunos, cuando por ejemplo el usuario final accede de forma directa a la fuente primaria.

En consecuencia y según hemos analizado, aumenta la problemática asociada y la ley se va configurando insuficiente en cuanto resulta escasa puesto que no regula de manera acabada esta especie de “posta” informática en el cual actores del mercado poseen un interés predominante, puesto que configura todo un sistema económico lucrativo, el cual obedece al perfilamiento del segmento o individuo objetivo, con diversas finalidades tales como mercantiles, políticos, estadísticos, etc.

II. Uso para incidir en procesos de decisión económica

a. Datos personales de carácter económico, financiero, bancario o comercial.

¹³⁵ Jervis, P., Op. cit. p. 159

¹³⁶ Op. cit. p.160

Debemos considerar en este apartado un doble aspecto: La ley lo trata en su artículo 4° en cuanto datos personales provenientes de fuentes accesibles al público, como una de las hipótesis en que no se requiere autorización del titular, constituyendo una excepción a la autorización previa expresa¹³⁷ y por tanto, tampoco exige que prime a su respecto el principio de finalidad¹³⁸.

Y por otro, la Ley dedica un apartado completo a la materia, en el Título III “De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial” arts. 17 a 19. Así, en palabras de Jervis, tal distinción que realiza la ley lo hace al referirse a los “datos patrimoniales negativos”¹³⁹, a los cuales hace referencia en este título, que atañen a la existencia de obligaciones o deudas. Es a este respecto que la ley no es clara, puesto que el ámbito de aplicación de la excepción es clave para su interpretación. ¿Se debe entender que sólo afecta a este tipo de datos, las obligaciones o deudas, puesto que los detalla de manera acabada, o debemos concluir que la excepción afecta tanto a aquellos como a los demás tipos de datos patrimoniales, no sólo respecto de las obligaciones? Las consecuencias sobre una u otra postura son radicales, y he ahí su importancia.

A juicio de Jervis, la excepción “abarca todo tipo de dato patrimonial, dado que el legislador no distingue, no pudiendo, en consecuencia, el intérprete distinguir y porque el Título III habla de obligaciones de carácter económico, financiero, bancario o comercial y la excepción se refiere a datos de carácter económico, financiero, bancario o comercial (sin mencionar que se trate de obligaciones), y por último, porque así lo pareció entender uno de los Senadores que participó activamente en la tramitación del proyecto de ley respectivo”¹⁴⁰

Así, se produce un fenómeno particular: “Se pueden tratar (...) datos patrimoniales negativos si este tratamiento ha sido autorizado por el titular (autorización

¹³⁷ In. 5° artículo 4 Ley 19.628 de 1999: “No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.”

¹³⁸ Art. 9 Op.cit.: “Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público”

¹³⁹ Jervis, P., Op. cit. p. 108

¹⁴⁰ Loc.cit.

convencional) o por la ley a través de la excepción de fuente accesible al público (autorización legal), sin embargo, algunos de estos datos (los que se encuentren fuera del listado que se contempla en el artículo 17¹⁴¹), no pueden ser comunicados, pero sí tratados”¹⁴²

En cuanto a los datos patrimoniales positivos, o sea los referidos a los activos patrimoniales, éstos cabrían en la excepción en comento si la fuente de la cual se extraen se entiende como de acceso público, o sea, no requieren la autorización de la persona titular para su tratamiento, y para el caso contrario, que provengan de una fuente reservada o privada, han de requerir autorización, sea de la ley o de su titular.

b. Datos necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Otra de las excepciones contempladas por el artículo 4° de la Ley hace referencia al llamado “Marketing Directo” o mercadotecnia directa, el que se entiende como una comunicación bidireccional¹⁴³ que utiliza bases de datos para configurar el perfil de su público objetivo o target, sea almacenando niveles de segmentación o individualizando a sus clientes, enviando comunicación directa y bidireccional en base a preferencias, gustos, edad, entre otros y por diversas vías, algunas más tradicionales como el telemarketing y otras más modernas como las redes sociales. A este respecto cabe entender que de igual manera la persona tiene a su favor la posibilidad tanto de solicitar la revocación de la autorización del tratamiento de datos personales, el bloqueo de sus datos y asimismo el derecho a oposición, según lo consagrado en el artículo 3° de la Ley¹⁴⁴.

¹⁴¹ Art. 17 Ley 19.623 de 1999: “Los responsables de los registros o bancos de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas consten en letras de cambio y pagarés protestados; cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales”

¹⁴² Jervis, P., Op. cit. p.114

¹⁴³ Cyberclick. *Marketing Directo. ¿Qué es el marketing directo? Ventajas y ejemplos.*
<https://www.cyberclick.es/marketing/marketing-directo>

¹⁴⁴ In. 2° art. 3 Ley 19.628 de 1999: “El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión”

Esta normativa ha sido criticada en diversas instancias, pues se comprende el carácter económico de lucro perseguido en la preservación de esta actividad al exceptuarla de la aplicación de los requerimientos y protección dada por la Ley¹⁴⁵,

III. Uso para fines electorales

a. Mercado de datos personales públicos.

Un aparentemente inocuo mercado de datos pertenece al caracterizado por Jarvis como el de identificación¹⁴⁶, donde figura el Estado como el mayor actor del mismo: “múltiples órganos públicos como el Registro Electoral, el Servicio de Impuestos Internos, y actualmente el Servicio de Registro Civil e identificación, venden los datos de identificación que poseen de los ciudadanos a través de la firma de contratos de prestación de servicios, a empresas que luego, utilizan esa información personal para usos propios, o bien, sirven de canales de distribución de los datos personales que compran. Todo lo anterior, a través de procesos automatizados de comunicación.”

Es así como el Servicio de Impuestos Internos (SII), la Tesorería General de la República (TGR), el Servicio de Registro Civil e Identificación (SRCI) y el Servicio Electoral (Serval) han indicado encontrarse facultados para realizar contratos y convenios de intercambio de información y asimismo el SRCI particularmente “vende directamente acceso a información personal de sus bases de datos a cualquier empresa que lo solicite y que cumpla con los requisitos técnicos y contractuales que el contrato de adhesión que creó el SRCI establece a estos efectos”¹⁴⁷

Como tal, no se ha configurado ningún ilícito puesto que las entidades disponen de la legitimidad brindada a los efectos, considerándose esas bases de datos como

¹⁴⁵ Jarvis, P., Op. cit. p. 111

¹⁴⁶ Op. cit. p. 174

¹⁴⁷ Op. cit. p. 185

registros públicos y siendo susceptibles de intercambio y cruce de las mismas con fines económico-comerciales¹⁴⁸.

b. Mercado de datos personales en Internet¹⁴⁹

Este mercado de datos ha ido en constante crecimiento, más aún con las condiciones de años pasados y actual de contingencia sanitaria global de confinamiento y boom de la utilización de la Red con diversos fines, tanto laborales, informativos, comerciales, sociales, etc.

Acá encontramos lo que se denomina “tratamiento invisible de datos personales”, lo cual engloba “un conjunto de operaciones y procedimientos técnicos efectuados por programas y equipos capaces de procesar los datos de los usuarios y ponerlos a disposición de terceros sin conocimiento o consentimiento de sus titulares”¹⁵⁰.

La persona, al navegar por internet, va dejando una huella aparentemente invisible pero cargada con sus datos personales, hábitos, preferencias, gustos, creencias y un largo etcétera de información personal, todos los cuales es recogido por diversas herramientas informáticas, en tanto aquellos datos brindados pueden haber sido otorgados de manera voluntaria por el usuario, como involuntaria mediante toda su actividad en web. Si así lo pensamos y queremos graficar, en este mismo acto de desarrollo y escritura de Proyecto de Memoria, hemos dejado una huella considerable respecto de intereses llenos de clicks diversos, orientados a la recopilación de información para desarrollar de manera acabada este Proyecto, todo lo cual se ha recopilado por los navegadores y agentes de Internet que rastrean tal actividad. Así, en el mismo acto y con el propósito de concluir nuestra ardua tarea académica, hemos sido perfiladas al mismo tiempo, por toda nuestra actividad, ya sean horarios, intereses, historial de búsqueda, páginas visitadas, enlaces seguidos, tiempo de estadía en cada sitio, páginas abiertas, páginas cerradas, documentos descargados, navegadores utilizados, equipo de conexión y así, un sinfín de información atractiva para los agentes quienes pueden

¹⁴⁸ Jervis, P., Op. cit. pp. 159-188

¹⁴⁹ Op. cit. pp. 174-180

¹⁵⁰ Op. cit. p. 174

ser destinatarios anónimos de nuestra información ofrecida por entes desconocidos o no, quienes no requieren necesariamente nuestra autorización para transar este volumen informativo ni las bases de datos asociadas. De esta manera, entre lo más común se pueden identificar herramientas informáticas como las cookies y los spyware o software de espionaje¹⁵¹

Al respecto, cabe recordar lo dicho respecto a los datos disociados o estadísticos, los que no estarían considerados en la aplicación de la Ley, al no considerarlos como datos personales puesto que no se asocian a persona determinada. En tal efecto, en cuanto la información recabada no pueda asociarse directamente a un individuo en particular, no estaría afecto su tratamiento a las distinciones de la Ley, sin embargo en cuanto herramientas informáticas, existen otros sistemas de trazabilidad e identidad, como los relativos a los números IP de los computadores, números que en condiciones de uso regular del aparato son fijos y estables, pudiendo a través de su localización y georeferencia, asociarse a un sector determinado dentro de un radio territorial específico. ¿A aquello entonces, no le correspondería el ser considerado como una identidad? algo quizás homologable a lo que es el Rut o Run de las personas, en cuanto usuario o individuo actor de la Red.

IV. La respuesta desde la combinación de aspectos de temas a abordar: Las neurociencias, la neuroética y los neuroderechos.

Un apartado relacionado a la vez que independiente constituye el campo de las neurociencias. La investigación neurocientífica se puede remontar a estudios de larga data en la historia del ser humano, pero que a través y de la mano de la evolución tecnológica moderna ha visto mayores avances y frutos como campo exploratorio en terrenos del Derecho. A todas luces, ha trascendido con mayor firmeza en la posteridad de los tiempos modernos sobre la doctrina y la investigación, puesto que en el trascendido de la experiencia vital es que se configura el Esquema Normativo y a su respecto, parece tener mucho que decirnos la investigación neuronal reciente.

Así nos comenta Eduardo Demetrio "(...) la moderna neurociencia -en su vertiente más radical, por supuesto- aduce haber verificado empíricamente el inexorable determinismo

¹⁵¹Op. cit. 176

cerebral, que operaría como una especie de jaula infranqueable de la conducta humana”¹⁵²

a. Las neurociencias

Representan “un conjunto de conocimientos que tienen por objeto el estudio del vínculo entre el cerebro y la conducta humana. (...) una ciencia interdisciplinar que busca aportar explicaciones del comportamiento de las personas en términos encefálicos, es decir, explicados por correlatos neurológicos presentes en el cerebro de cada una de las personas”¹⁵³

Por tanto, en la modernidad hemos logrado comprender que el cerebro humano no es un mecanismo preformado y estático, sino que es un muy complejo órgano funcional adaptativo que en tanto flexible y funcional, opera en función de la supervivencia y adaptación correlativa al ambiente y medio en que se desenvuelve el individuo, logrando en el ser humano una cúspide evolutiva que nos hace capaces de procesar constantemente nuestro entorno y la información que de él percibimos, pasando por un muy subjetivo procesamiento de aquellos datos para así confluir en una reacción posterior a los mismos. Todo lo cual opera de manera más o menos consciente, comandando tanto funciones autónomas vitales como elaborados procesos de inferencia y deducción racional ante las situaciones del día a día. Así, concluyen algunos¹⁵⁴ que derivado de este proceso adaptativo, el sujeto no dispondría de “libertad en sus respuestas ante las diversas situaciones, sino que ya estuviera condicionado por las reacciones que su cerebro va creando como consecuencia de esa necesidad adaptativa”. Por tanto, la voluntad y libre albedrío serían más bien una consecuencia de un sistema ya procesado, evaluado y automatizado de respuesta y no cabría entonces más que considerar al individuo como expresión de sus impulsos fisiológicos creados desde el momento de su nacimiento. Así, sus reacciones estarían condicionadas ex ante por sus vivencias y adaptaciones cerebrales, así cuanto también serían el reflejo de sus propias incapacidades del órgano; de esta forma se ha ido conformando una especie de

¹⁵² Demetrio Crespo, E., (2017). *Fragmentos sobre neurociencias y derecho penal*. Ed. B de F. p. 9

¹⁵³ Acevedo, N. (2015). *Culpabilidad jurídico penal y neurociencias: una aproximación multidisciplinaria a la fundamentación y justificación de la culpabilidad frente a los actuales avances científicos*. [Memoria para optar al grado de Licenciado en Ciencias Jurídicas, Universidad de Chile]. p. 13

¹⁵⁴ Nieva, J. (2016) *La ciencia jurisdiccional, novedad y tradición*. Marcial Poin. p. 679

neodeterminismo¹⁵⁵, bajo el cual se concluye que la voluntad y la expresión del yo serían simples ilusiones, siendo el cerebro el responsable, desde un primer momento, de ejecutar las decisiones.

En consecuencia, se ha captado que en un estadio inicial, confrontado el sujeto a un hecho determinado, la reacción desde el campo neurocientífico se identifica en una etapa preliminar inconsciente que luego el agente es capaz de captar de manera racional, de tal modo que sería indistinguible un proceso “voluntario” en todo aquello, sino más bien configuraría una “sensación” de voluntad. Todo lo cual expresa Nieva, constituye más bien un fenómeno de discusión filosófica más que científica, lo cual reduce a la conversación a un discurso más bien argumentativo. Por lo pronto, el ámbito que nos convoca necesariamente ha de tener en cuenta lo que la neurociencia le puede aportar, pues es el ámbito del proceso neuronal y la toma de decisiones el hito relevante que buscamos analizar. Es en suma, objetivo de la neurociencia el conciliar o intentar dar respuesta a preguntas profundas que desde antaño se realiza la humanidad, como lo es lo relacionado a las bases de la libertad, de la autonomía, de la toma de decisiones, o bien, en su contrapartida, ¿Cuán delimitada e inmutable se encuentra la personalidad humana? ¿Resulta acaso que hemos faltado en nuestra investigación, dejando de lado e ignorando a un órgano al parecer tan simple a la vez que tan complejo, y que no debiera permanecer oculto en toda esta discusión?

¹⁵⁵ Nieva, J., Op.cit. p. 680

b. La neuroética.

En el desarrollo y avance de la neurociencia, se percibe de evidente manifiesto las implicancias éticas que aquello podría conllevar. ¿Resulta inocua la investigación cerebral en el sujeto en estudio? ¿Hasta dónde debe trazar su camino la ciencia en pos del objetivo científico? En tal caso es que se ha puesto la neuroética, la cual define y cita Acevedo, “como ‘el estudio de las cuestiones éticas, legales y sociales que surgen cuando los descubrimientos científicos acerca del cerebro se llevan a la práctica médica, las interpretaciones legales y las políticas sanitarias y sociales’”¹⁵⁶.

Ante lo cual advierte, “[l]as Neurociencias interferirían con las intuiciones que tenemos sobre la responsabilidad y la culpabilidad, que constituyen la base de nuestra sociedad (...) la importancia de los problemas éticos a los que dan lugar las Neurociencias, sobrepasan aquellos relacionados en la genética”¹⁵⁷. Así, el cambio paradigmático puede ser rotundo, tanto o más como la afectación del individuo en particular, puesto que el avance en las investigaciones neurocientíficas pueden llevar a un futuro con alcances insospechados, imposibles de prever en nuestro tiempo, ya que como vimos no se limitan únicamente a cierta forma de concebir o experimentar con el cerebro y sus procesos, puesto que el funcionamiento de éste obedece a un sistema complejo e interconectado, tanto de estímulos exteriores de todo tipo (químico, físico, ambiental en general) como estímulos internos (balances hormonales, minerales, tiempos de descanso, alimentación, etc), todo lo cual lleva aparejado una serie de dilemas éticos que las neurociencias deben plantearse y resolver a la luz de las consideraciones en el campo de la neuroética, sin dudas.

¹⁵⁶ Acevedo, N. Op. cit., p. 38. Citando a Sánchez-Migallón, S. y Giménez, J., *Neuroética. Philosophica: Enciclopedia filosófica on line.* (7 de junio de 2015)

<http://www.philosophica.info/voces/neuroetica/Neuroetica.html>

¹⁵⁷ Acevedo, N. Op. cit., p. 35. Citando a Fuchs, T., ((2006). *Ethical issues in neuroscience. Current Opinion in Psychiatry* 19: 600.

c. Los neuroderechos

En el campo de los neuroderechos debemos realizar una distinción previa y precisar qué entenderemos por aquellos.

Así, como se refiere en el artículo en *El Mostrador*¹⁵⁸, el que servirá de base para la discusión sucinta en esta materia, podemos distinguir el anglicismo *neurolaw* referido a “la relación entre derecho y neurociencias”. Y, separadamente, *neurorights*, referido a una carta de derechos moderna, o “nuevos” derechos, producto del avance de las tecnologías y en específico, de la implicancia de la investigación de las neurociencias y su alcance y efectos en el individuo. Así y sobre esta categoría, se discute si es menester afianzar una nueva terminología y agregar quizás, una nueva tipología de DD.HH. que ponga énfasis en la protección y resguardo específico de intereses primordiales para el ser humano en esta era tecnologizada y neurocientífica. De esta forma, se plantea que “[u]na nueva categoría de DDHH debe necesariamente ser consistente, no repetitiva, precisa, de alto consenso internacional (...) ‘Las neurotecnologías son disruptivas o podrían serlo porque alteran tradicionales concepciones de identidad, agencia, privacidad (Goering, S., Klein, E., Specker Sullivan, L. *et al.* (2021).’”

Para efectos de este estudio, nos abocaremos a esta segunda temática relacionada, ya que para el año 2020, ingresa a tramitación en nuestro país el Proyecto de Ley *Sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías*¹⁵⁹, mediante el cual se promueve la inclusión de cinco nuevos derechos o neuroderechos, que a saber serían:

- Derecho a la privacidad mental (los datos cerebrales de las personas)
- Derecho a la identidad y autonomía personal
- Derecho al libre albedrío y a la autodeterminación

¹⁵⁸ Cornejo, M., El Mostrador (26 de julio de 2021). *Neuroderechos y neurotecnologías en Chile: Prioridades legislativas* <https://www.elmostrador.cl/noticias/opinion/columnas/2021/07/26/neuroderechos-y-neurotecnologias-en-chile-prioridades-legislativas/>

¹⁵⁹ Chahuán, F., Coloma, J., De Urresti, A., Girardi, G., Goic, C. (7 de octubre de 2020). Proyecto de Ley Boletín N° 13828-19. *Sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías* [en segundo trámite constitucional]. <https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=14385&prmBOLETIN=13828-19>

- Derecho al acceso equitativo a la aumentación cognitiva (para evitar producir inequidades)
- Derecho a la protección de sesgos de algoritmos o procesos automatizados de toma de decisiones

De aquellos, se discute si requieren en suma una consagración en la Carta Fundamental mediante su reconocimiento como nuevas categorías de derechos o bien, resulta prioritaria una adaptación y actualización de lo que se comprende dentro del catálogo ya consagrado como garantías fundamentales. Asimismo, se debe determinar a qué tipo de avance nos estamos refiriendo, puesto que en la actualidad conviven los avances de la neurociencia terapéutica y con fines de restauración de la salud, sin mayores inconvenientes respecto a las garantías ya establecidas. Más conviene hacernos algunos cuestionamientos mayores respecto a las materias en revisión. ¿Puede el derecho a la privacidad o protección de datos personales subsumir la protección a la privacidad mental? ¿o debe considerarse el acápite particular de datos neuronales como una categoría autónoma?

En opinión de Cornejo (2020):

“(...) quizá la protección de una categoría interesante, los neurodatos, de los cuales se puede extraer información confidencial por ser datos sensibles, deban tener un resguardo específico y el proyecto de ley de neuroderechos logre este cometido, sobre todo por los insospechados usos que la inteligencia artificial pueda hacer con ellos. Queda la pregunta si un buen sistema de protección de datos no es suficiente para proteger a la persona de intromisiones a su privacidad, sea esta mental en concreto o bien figurativamente hablando. Quizá un doble candado (ley de neuroderechos más ley de protección de datos) realmente logre mayor protección de la intimidad de las personas de cara a los desarrollos neurotecnocientíficos.”

Respecto a los derechos a la identidad, autonomía personal, libre albedrío y autodeterminación, previamente avizoramos que algunos partidarios de las neurociencias optan por la teoría del determinismo y en suma, aseveran la

falsedad o ilusión en cuanto la existencia de la voluntad autónoma en sí misma, debido al intrincado mundo del inconsciente cerebral, el que opera en casos probados ex ante respecto a las consideraciones conscientes del sujeto en estudio. Sin embargo, aquello no ha podido demostrar ser más que una casuística y no una generalidad, la cual quizás conllevaría a un replanteamiento del sistema normativo, pero que de momento, no ha logrado avanzar más allá de argumentos filosóficos aplicados al campo neurocientífico. Cosa que sin duda vale cuestionarse en la actualidad pero que posiblemente pueda entenderse que no requieren una categorización en la carta fundamental puesto que caben garantías que les puedan subsumir, además que la determinación por ejemplo, de los límites a la autodeterminación y por ende, su protección, quede en un primer momento planteado de forma demasiado abierta y sujeto a muy diversas concepciones de lo que en el sujeto en particular se refiera tal concepto, obedeciendo más bien a su sistema de crianza, valórico, educacional, etc. cosa que ya puede resguardar desde otras veredas del sistema normativo.

En cuanto al derecho equitativo a la aumentación cognitiva y al derecho a la protección de sesgos de algoritmos o procesos automatizados en la toma de decisiones, podrían representar un avance en esta nueva categoría, sobretodo en el campo de la aumentación cognitiva ya que más allá de los usos médico-terapéuticos en pos de la recuperación de la salud, el individuo puede operar más allá y proceder a los aumentos en funciones específicas y accesorias a su condición humana, pero que redunden en una mejora exponencial respecto del común de las personas, puede efectivamente generar injusticia, inequidad e incluso una nueva categoría de seres humanos aumentados, quienes por medio de sus recursos económicos obtengan mejoras significativas a la condición humana. De una manera más gráficamente representado, si el sujeto A obtuviera brazos adicionales o bien una estructura extracorpórea que mejore su fuerza y rendimiento físico, al confrontar al sujeto B por oportunidades laborales o de cualquier índole en que incida tal categoría, como por ejemplo, deportes, claramente se verá con una situación en extremo ventajosa frente al sujeto B que no ha podido acceder a aquellas mejoras, y tanto así, que quienes deseen, incluso teniendo los recursos económicos a su alcance, permanecer sin estas mejoras, se pueden ver enfrentados a la exclusión y marginamiento social, por el simple ánimo

de estar satisfechos con sus cualidades biológicas de nacimiento. Y respecto a la protección de sesgos de algoritmos, íntimamente ligado a la protección de datos personales y protección de datos cerebrales (que habrían de considerarse como una categoría dentro de los datos sensibles) la manipulación de estos datos ciertamente podría conllevar discriminaciones arbitrarias e incluso ser posible la manipulación de un tercero sobre el proceso de toma de decisión de los individuos, suprimiendo la libertad, la autonomía y el libre albedrío.

Así también advierte Acevedo (2015, p. 14), citando a Slachevsky (2007), que las “(...) técnicas de neuroimagen o de resonancia magnética funcional o nuclear (RM o Fmri) pueden alcanzar un nivel de complejidad tan alto que incluso permitirían revelar el pensamiento de cada persona, vulnerando la privacidad mental”. De esta forma, se erigiría el *neuromarketing* en términos de uso comercial y ventas o bien en materia judicial se podría tener un uso probable en “la detección de mentiras, la que permitiría en un futuro identificar el “conocimiento culpable” mediante la asociación de elementos vinculados a un crimen con la reacción que puede provocar en una determinada persona” (en cita a Farah, M., p.34-35. Acevedo p.14) o bien en materia de rehabilitación de los condenados, y así, un vasto horizonte de posibilidades de aplicación de los avances neurocientíficos, de consecuencias que ya no parecen ni tan lejanas ni tan intrascendentes.

CAPITULO V. LO AFECTADO DESDE LA TEORÍA DEL BIEN JURÍDICO

I. Los riesgos de no regular

Como hemos desarrollado a lo largo de este trabajo, el avance e incorporación de las nuevas tecnologías, junto con el nacimiento de la sociedad de la información, trajo consigo pugnas irremediables de derechos. Tal como lo señala Pérez Luño,

“En la situación tecnológica propia de la sociedad contemporánea todos los ciudadanos, desde su nacimiento, se hallan expuestos a violaciones de su intimidad perpetradas por determinados abusos de la informática y la telemática. La injerencia del ordenador en las diversas esferas y en el tejido de las relaciones que conforman la vida cotidiana se hace cada vez más extendida, más difusa, más implacable. Esta proyección de los efectos del uso de la informática sobre la identidad y dignidad humanas, incide también en el disfrute de los valores de la libertad y de la igualdad. La libertad, en las sociedades más avanzadas, se halla acechada por el empleo de técnicas informáticas de control individual y colectivo que comprometen o erosionan gravemente su práctica. Contemporáneamente se produce una agresión a la igualdad, más implacable que en cualquier otro período histórico, desde el momento en que se desarrolla una profunda disparidad entre quienes poseen, o tiene acceso, al poder informático y quienes se hallan marginados de su disfrute”¹⁶⁰.

La constante sobreexposición a la que se ven expuestos los usuarios de la web, permite apreciar que los bienes jurídicos que se encuentran siendo vulnerados ya no solo se refieren a los aspectos de la “intimidad o la protección de los datos personales (...) sino que también se afectan todas las libertades y dignidad humana en general”¹⁶¹.

Así las cosas, Suñé Llinás es de la opinión de que “existe una importante tensión entre dos grandes valores: libertad de información y protección de la intimidad y demás derechos y libertades fundamentales frente a ella, sobre todo cuando se dispone de datos muy abundantes sobre las personas, gracias a los sistemas informáticos, y se emplean a

¹⁶⁰ Del Fierro, op. cit. pp. 43-44. Citando a Pérez, A. (2006). *La Tercera Generación de Derechos Humanos. Aranzadi*. p.31.

¹⁶¹Op. cit. p.44.

fondo las posibilidades que éstos dan, en cuanto a interconexión de ficheros”¹⁶². Esto quiere decir que nos encontramos frente a derechos que se van a mantener en una pugna constante, y donde para analizar cuál primaría en desmedro del otro, se debería analizar el caso concreto. Pero la situación antes descrita es totalmente irreal, ya que nos encontramos en presencia de una red digital con miles de millones de usuarios en que cada uno es un caso concreto, y por ello, es tan dificultoso legislar y establecer leyes generales aplicables a los distintos ordenamientos jurídicos. La importancia, finalmente, no radica en analizar caso a caso sino en establecer políticas comunes, cláusulas de responsabilidad efectivas y un planteamiento global desde el entendimiento de las diferencias, partiendo de la base de que las redes sociales ahora son parte intrínseca de las personas y sin ellas, no se podría hablar de un desarrollo íntegro de la persona.

Vienen a reforzar la idea recién planteada, los autores Pérez Luño y Suñé Llinás al concordar “en que el principal derecho afectado por el avance de las nuevas tecnologías de la información es el derecho a la intimidad, pero al mismo tiempo reconocen que como consecuencia de afectación, se ven afectados el resto de los derechos y libertades fundamentales de la persona, produciendo efectos negativos incluso sobre la identidad y dignidad humana”¹⁶³.

II. La posible necesidad de una intervención del derecho penal. Hacia una regulación global.

Confrontado el Derecho frente a las diversas miradas de la realidad actual, en particular nos merece especial atención el campo de la neurociencia en relación al Derecho Penal y la problemática suscitada en atención a los presupuestos base del Derecho mismo.

Buscaremos entonces acercarnos a la discusión de la manera más integradora posible, siempre en atención que para mayor detalle y abundamiento, solicitamos al lector se pueda referir a las obras citadas a continuación, las que hacen ejemplar descripción y detalle sobre la materia objeto de este acápite.

Dicho lo anterior y según nos relata Demetrio Crespo a lo largo de su obra¹⁶⁴, a la luz de la neurociencia, pareciera perder sentido el concepto tradicional de indeterminismo

¹⁶² Del Fierro, Loc. cit. Citando a Suñé, E. (2002). *Tratado de Derecho Informático* (Vol. 1). Madrid: Universidad Complutense Madrid. p. 16.

¹⁶³ Op. cit. p.44.

¹⁶⁴ Demetrio Crespo, E., Op.cit p. 19-74

volitivo, puesto que el avance científico ha configurado a la voluntad como un mero hecho anterior al procesamiento consciente del cerebro de dicha toma de decisión, por cuanto cobra mayor valor y fuerza para la visión neurocientífica, la cual prefiere indicar al determinismo como regla en la materia, así, en su opinión “es importante no perder de vista que la carga de la justificación del castigo recae de quien afirma su legitimidad y que por tanto no es posible ‘pasar de puntillas’ cuando se trata de averiguaciones acerca de los condicionantes en que tiene lugar el comportamiento humano que consideramos culpable.”¹⁶⁵ .

Siguiendo con el planteamiento neurocientífico, Acevedo nos grafica (citando a Leyton J., 2014)¹⁶⁶ “en el hombre no hay y nunca hubo libertad, sino que estaríamos determinados en nuestros comportamientos por procesos que no podemos controlar y de los que por tanto, no seríamos responsables. Se retrocederían así los años de discusión – aparentemente ya superados- en torno al debate entre determinismo y libre albedrío.” En consecuencia, cabe cuestionarse (citando a Luzón P., 2012) “¿Tiene razón la sociedad, y en su caso el Derecho que consideran que ciertos sujetos deciden y actúan libremente, y como consecuencia de ello pueden merecer un reproche jurídico penal? ¿O está equivocada la sociedad y el Derecho, pues la libertad es un espejismo o fantasía social, y todos estamos determinados por factores externos e impulsos inconscientes que no podemos controlar? ¿Son dignas de alabanza o reproche las acciones humanas o somos títeres en manos del destino o el azar? ¿Es empíricamente demostrable la libertad?”¹⁶⁷ Ciertamente, responder tales cuestionamientos ya sería obra de un proyecto independiente al que nos convoca, pero para dilucidar de cierta manera una posible respuesta, seguimos a Demetrio Crespo cuando, al citar a Prinz (2017, p.29-30), nos conduce hacia un posible ángulo con la yuxtaposición entre ‘el determinismo en la realidad y la libertad en la percepción’, dando cuenta del fenómeno dual que puede representar la libertad, en un sentido real objetivo determinado, mientras que un plano psicológico, como impulso o percepción subjetiva de las decisiones llamadas como voluntarias por el sujeto, momento en el cual sucede una valoración de la acción por el individuo. Así las cosas, se edifica a la voluntad como una *institución social* (Prinz, 2004. Citado por Demetrio Crespo, 2017, p.31). Pues tenemos de este modo conculcados, a la

¹⁶⁵ Op.cit. p. 22

¹⁶⁶ Acevedo, N., Op. cit. p.141

¹⁶⁷ Op. cit. p.144

luz de las neurociencias, los conceptos clásicos de libertad, voluntad, libre albedrío, autodeterminación y en ulterior instancia, la responsabilidad y la culpabilidad, puesto que si aceptamos el determinismo como base para evaluar las acciones, entonces, ¿de qué forma cabría la responsabilidad o culpa del individuo dentro de un proceso que no le empeece? ¿Cómo puede estructurarse un proceso de valoración moral en el sujeto si la voluntad es una “mera ilusión y el mal un fenómeno biológico que reside en el cerebro”¹⁶⁸? puesto que consideradas así las cosas, ya lo indicaba el autor previamente, tampoco puede pasarse por alto esta discusión que es del todo relevante para el Derecho Penal tal y como se concibe en la actualidad y tradicionalmente, lo cual no obsta a su vez para provocar una nueva conceptualización, armonizada probablemente con las luces del comportamiento humano en su esfera biológica que nos pueda entregar la neurociencia. Continúa así en esta línea, al ofrecer una *tercera salida*- en esta confrontación entre el determinismo e indeterminismo- y nos plantea el *agnosticismo*¹⁶⁹, que al citar a Roxin (2011, p.868 y ss.), nos conceptualiza que se debe “entender la culpabilidad como el ‘comportamiento injusto a pesar de la asequibilidad normativa’, lo cual “cuando se da esta asequibilidad normativa, se parte, sin poder ni querer demostrarlo en el sentido de la libertad de voluntad, de que el autor también tiene la capacidad de comportarse según la norma, por lo que se convierte (automáticamente) en culpable cuando no opta por ninguna de las alternativas de comportamiento que le son accesibles psíquicamente”. Así, con esta *presunción de libertad* los indeterministas pudieran estar de acuerdo, ya que se configura una “posición normativa, una regla de juego social, cuyo valor social es, (...) independiente del problema de la teoría del conocimiento y de las ciencias de la naturaleza de la libertad de voluntad”. Sin embargo, es en razón de lo discutible de esta última parte que algunos autores como Jakobs han desvinculado “totalmente su concepto de culpabilidad de cualquier suposición de libertad”. Así, citando a Jakobs (p.61) “se considera culpable a aquel delincuente cuya penalización resulta necesaria para conseguir el fin social que se persigue, sea la intimidación de futuros delincuentes o el restablecimiento de la quebrantada confianza de la generalidad en la vigencia de las normas y la inviolabilidad de los bienes jurídicos”. De este modo, va concluyendo el autor y citando a Vives Antón (2002, p. 32), “¿Hasta dónde puede llegar la duda determinista?” en opinión del referido tal duda ‘no se limita a poner en tela de juicio la culpabilidad, sino

¹⁶⁸ Demetrio Crespo, E., Op.cit. p. 63

¹⁶⁹ Op. cit. p. 60

que involuntariamente va mucho más allá: todo el lenguaje de la acción quedaría deslegitimado por ella’.

Y es respecto a esto lo que nos alerta a su vez que, a la luz de estas dilucidaciones, si este reformado concepto de libertad y voluntad obedecieren a una valoración que nace en parte desde un fenómeno biológico, en parte a un fenómeno social o quizás constructo normativo, cierto es que, y volviendo al tema central de nuestra discusión, inusitadas consecuencias puede aparejar la manipulación externa del órgano encefálico por medios tecnológicos creados con tales fines, pues es fácilmente suponer que el sujeto bien puede ser objeto de manipulaciones intencionadas (o mal intencionadas, da igual el sentido), perdiendo por completo el carácter volitivo en la determinación de sus acciones, por lo que las bases del sistema punitivo se verían tambalear en el entendido que el sujeto es imputable en la medida que sus acciones vayan aparejadas de, a lo menos, conciencia, valoración o la representación de los efectos que aquellas pudieren causar en los otros individuos. Así y yendo un poco más allá, incluso nos podríamos representar, una posible evolución hacia la mera instrumentalidad del ser humano, ya incapaz de percibir la realidad de un modo suficiente que le permita realizar los juicios de valor necesarios para la comprensión de la trascendencia de sus actos, habiéndose dado plena cabida a la concepción falsa o ilusoria de los conceptos de libertad y voluntad. De suerte que por ahora - o mientras tanto- las neurociencias no han logrado refutar de manera general e indubitable la concepción indeterminista del Derecho Penal, por cuanto y aunque la respuesta no es unívoca, hemos quizás de asistir a la reestructuración del Derecho en la medida que le conocemos actualmente, o quien sabe, todo esto no quede en una mera discusión de carácter doctrinario y las neurociencias no sean capaces, ni ahora ni en el futuro, de entregar las pruebas suficientes para el completo rechazo a la concepción de la libertad y voluntad indeterminadas.

III. La manipulación de los procesos decisorios y la contravención a la garantía constitucional de configurar libremente el plan de vida (la dirigibilidad de la conciencia y los procesos decisorios)

Ya analizado el campo de las neurotecnologías en relación al Derecho Penal y visto hacia dónde van encaminados los esfuerzos de la evolución humana, nos es dable comprender que tal como ha quedado de manifiesto, la existencia de un cuantioso y económicamente rentable mercado de datos personales, constatada su existencia y amparo legal, volviendo muy concretos los posibles avances en el campo de las neurociencias y la investigación del proceso del pensamiento. Por cuanto ya no parece tan distópico el futuro donde chips intracraneales y nanotecnología afecten al órgano cerebral y sus procesos biológicos, convergiendo simultáneamente la realidad *real* con la realidad *informática*, en un todo de existencia ya no dual, sino que complementario y estatuyéndose asimismo como parte integrante del proceso identitario de los individuos.

Por otra parte y para graficar, en su correlato noticioso actual, Elon Musk, el magnate millonario dueño de la empresa Tesla, y de la mano de su empresa biotecnológica *Neuralink*, estiman como 2022 el año en que puedan comenzar las pruebas de microchips neuronales en seres humanos, ya habiendo sido probado en cerdos y un mono macaco, con total éxito, según aseveró el fundador¹⁷⁰. Su interés es el de lograr “*sustituir* neuronas defectuosas o ausentes ‘tendiendo un puente’ entre las señales neuronales existentes”. No deja de ser menor que tales anuncios se han viralizado mediante la plataforma informática Twitter. Manifestación que ya entendemos, conlleva repercusiones mayores, siendo considerada como una fuente legítima en la publicación de los hallazgos así como de las intenciones del magnate y las repercusiones económicas globales. A mayor abundamiento, tales repercusiones se pudieron evidenciar con lo sucedido con la criptomoneda Dogecoin, la cual, con el abierto y público apoyo del magnate, “ha subido casi un 10,000% desde octubre de 2020 y se ha puesto en el top ten de las criptomonedas, ayudado por la extravagante personalidad de Twitter de Musk. A modo de comparación, bitcoin ha agregado un 400% en los últimos 12 meses”¹⁷¹. Sin embargo,

¹⁷⁰ Mike Blake. RT (8 de Diciembre de 2021). *Neuralink apunta al cerebro humano: Elon Musk anuncia pruebas para incrustar microchips neuronales en personas en 2022*
<https://actualidad.rt.com/actualidad/412955-elon-musk-anuncia-pruebas-humanos-neuralink>

¹⁷¹ Bambrough, B., Forbes (28 de Octubre de 2021). *La razón por la que Elon Musk apoya Dogecoin y no Shiba Inu, Bitcoin o Ethereum* <https://forbes.es/criptomonedas/122821/la-razon-por-la-que-elon-musk-apoya-dogecoin-y-no-shiba-inu-bitcoin-o-ethereum/>

tiempo atrás, derivado de su aparición en un reconocido programa estadounidense, sus dichos provocaron la caída estrepitosa de la divisa producto de sus comentarios ambiguos al respecto y sobretodo producto de haberla calificado como un “timo”¹⁷², lo cual nuevame pone en evidencia que si este es el poder que puede tener un agente individual, imaginemos entonces cómo ha de girar la brújula en cuanto sean mayores las tecnologías pudiendo integrarse estos dispositivos de manera biológica.

Por otra parte, en materia comercial nos referimos previamente al *neuromarketing*, la cual aprovecha los avances neurocientíficos para “permitir a las marcas saber cómo podían aprovechar este recurso para conseguir mayor número de clientes”¹⁷³, además de tratar de “comprender los procesos de decisión cerebrales que nos llevan a la compra de un determinado producto.”

Paralelamente, la compañía *Visión Integral*¹⁷⁴ ofrece el trabajo conjunto de la psicología y la neurotecnología para el tratamiento de condiciones como el estrés, la depresión, la ansiedad, los problemas de autoestima o el conflicto personal producido por una ruptura amorosa, entre otras afecciones, mediante el trabajo con aparatos estimuladores de ciertos puntos en la región encefálica además del tratamiento psicológico asociado.

En otro aspecto, las neurociencias exploran los neurofármacos, que a la postre podemos conceptualizar en los *nootrópicos*, tipos de “compuestos que se consumen para provocar en el cerebro un efecto determinado, mejorando y potenciando su rendimiento”¹⁷⁵, así, buscan “(...) provocar la aludida mejora cognitiva, los procesos generados por los nootrópicos guardan una estrecha relación en ciertos aspectos como el aumento de la síntesis de acetilcolina, un neurotransmisor que juega un destacado rol en la conexiones entre mente-músculo y que da lugar a una mejora en la coordinación”. De esta manera se han popularizado como estimuladores de los neurotransmisores, más eficientes y con menores efectos secundarios que otros compuestos que son considerados medicamentos.

¹⁷² Efe. Cotizalia (10 de Mayo de 2021). *El dogecoin cae un 30% después de que Elon Musk bromee con que "es un timo"*

https://www.elconfidencial.com/mercados/2021-05-10/dogecoin-caida-elon-musk-programa_3072099/

¹⁷³ Cerrilo, C. Occam (17 de Mayo de 2021) *Ejemplos y estrategias del neuromarketing.*

<https://www.occamagenciadigital.com/blog/ejemplos-y-estrategias-del-neuromarketing>

¹⁷⁴ Vision Integral, en: <https://visionintegral.org/>

¹⁷⁵ Colomer, J., HSN Blog (16 de Enero de 2020). *Nootrópicos para Potenciar la Inteligencia.*

<https://www.hsnstore.com/blog/suplementos/concentracion-memoria/nootropicos/>

Así, hacemos mención a todo lo anterior para graficar cómo el campo exploratorio del cerebro no descansa y ya desde ahí cabría preguntarnos acerca de la necesidad de precaver o no, por parte del Derecho, las posibles implicancias de estas situaciones, debiendo estatuir quizás, los neuroderechos como garantías fundamentales por ejemplo, o bien debiendo fortalecer el campo regulatorio actual, aunque sabido es la fuerte presión ejercida por parte de los agentes interesados del mercado en que la situación normativa continúe tal y como se encuentra hoy.

De esta manera podemos ya configurar un ámbito de acción donde el sujeto ha ido paulatinamente perdiendo posibilidad y campo para las decisiones de autodeterminación e identidad, pasando incluso por quienes esgrimen la inexistencia de la voluntad real, autónoma y libre del individuo sino más bien es manifestación de un proceso cerebral químico-eléctrico previo a las decisiones, base del concepto determinista que enlaza a la concepción neurocientífica en relación con la voluntad y la libertad.

CONCLUSIONES

A lo largo del desarrollo de este trabajo, hemos podido plantear al lector diferentes inquietudes respecto del tratamiento y el uso de los datos personales. Fuimos introduciendo el tema desde la revisión de los tipos de información que circulan en la web, la integración de las redes sociales en línea -entre las estudiadas- Facebook y Twitter, el nacimiento de la huella digital, la autodeterminación y por supuesto la normativa chilena desde el punto de vista de la Ley 19.628 sobre protección de la vida privada, la Constitución y otras normativas afines.

En tales circunstancias, y como pudimos observar, el usuario se va desarrollando en un ambiente real y virtual en lo que pareciera una dicotomía identitaria. Pero que sin embargo, y a diferencia de lo que sucede en la cotidianeidad del entorno real, en este mundo virtual sus intereses han sido recopilados, tratados, transmitidos, difundidos y posiblemente expuestos. Su información como usuario ha sido continuamente perfilada, su multiplicidad de clic en la web, el posicionamiento del puntero del ratón, el tiempo transcurrido navegando, sus horarios, las descargas, las páginas visitadas y así, un inimaginable etcétera de datos que son recabados y se van acumulando en una -para él imperceptible- huella digital que puede parecer carente de atractivo, pero que sin embargo para terceros reviste el mayor de los intereses. Porque aun sin saberlo, el usuario se posiciona en la mesa de transacción de datos y lamentablemente, con mayor o menor conciencia de aquello, continuamente va transando lo más propio e intrínseco de él: su identidad.

Llegado este punto, pareciera venir a su rescate la legislación previamente estudiada, pero que a la luz del cruce de circunstancias conexas, hemos podido entrever el cómo persiste y persevera la desprotección del sujeto, puesto que en el vasto universo de internet, los mecanismos de protección y control no parecen siquiera rozar la superficie de todas las implicancias y aristas que reviste el uso de la web. Lo cual pareciera a veces - y poniéndonos suspicaces- tener más ribetes de voluntariedad que de falta de posibilidad de previsión por parte del legislador.

Con todo, cabe seguir cuestionándonos y repreguntarnos ¿Nada puede hacerse ante las continuas faltas de la ley? ¿Se necesitará entonces, un nuevo estatuto de normas que se haga cargo efectivamente de la materia, o bien, lo que estamos añorando es un robustecimiento de la normativa ya en vigor?. Recordemos que en la finitud de los

recursos, pensar en requerir una acción de un agente que se ubica al otro lado del mundo resulta de sólo pensarlo, engorroso y caro.

Sin embargo, estos cuestionamientos por medio del desarrollo de esta memoria y caminando de la mano por esta senda que llamamos web, hemos encontrado un nicho en el cual los usuarios podemos manifestarnos, del que nos hemos apropiado y nos aventuramos a reconocer con ello, que el sujeto ya no sólo posee existencia en el plano biológico-físico, sino que se está configurando la construcción de su propia identidad en un ambiente dual de existencia. Pues si reconocemos esta parte de autodeterminación del individuo en las redes, podremos seguir avanzando hacia el camino del reconocimiento y aceptación que planteamos: UNA NUEVA CONCEPCION DE SER HUMANO. Del cual ya no es posible desprender y renunciar a las tecnologías e incluso en su faceta más íntima, las redes sociales se posicionan como lugar de morada, habitáculo personal desde el cual se desenvuelve el sujeto hacia la conexión con sus pares, en un universo cifrado en números.

Así las cosas, es posible comprender ya de mejor manera, que en este camino no hay vuelta atrás, las tecnologías cada día van creciendo y compenetrándose a pasos agigantados con el usuario, y en ese entendido, asistimos a la posición extrema de que ya no es posible comprender al individuo ajeno a las tecnologías, pretendiendo que es una opción viable el renunciar a ellas por no prestar por parte del agente de soporte o dueño de las plataformas suficiente garantía de protección y uso responsable de los datos obtenidos, es a lo menos, *naif*. Observamos en consecuencia, que el paradigma de concepción del ser humano ha de sincerarse y de realizar un ejercicio de apropiación y manifestación de la realidad virtual, pues solo así podremos propender a una adecuada legislación, más robusta o bien innovadora, donde se pueda construir una normativa que vele más eficientemente por el respeto a las garantías individuales y donde ya no se conciba que la absoluta responsabilidad de uso recaerá en los usuarios.

Finalmente, todo el ejercicio desarrollado a lo largo de estas páginas ha sido encaminado a poder otorgar una visión complementaria e integrativa de la situación actual, y que si bien no hemos podido explayarnos *in extenso* acerca de cada una de las temáticas aquí expuestas, lo cual fácilmente correspondería a documentos completos separados según materia, sí esperamos haber conseguido el efecto de despertar la curiosidad y el pensamiento crítico, haciéndonos cargo de que las problemáticas planteadas están lejos

de tener una solución pronta y unívoca, pero que en el cometido de estudiar la materia objeto de este Proyecto de Memoria de Prueba, hemos podido evidenciar y analizar la problemática al amparo del Derecho y nuestra situación jurídica nacional actual.

BIBLIOGRAFÍA

AUTORES.

1. ACEVEDO VEGA, NICOLÁS. *Culpabilidad jurídico penal y neurociencias: una aproximación multidisciplinaria a la fundamentación y justificación de la culpabilidad frente a los actuales avances científicos*. [Memoria para optar al grado de Licenciado en Ciencias Jurídicas, Universidad de Chile, Santiago] URI: <http://repositorio.uchile.cl/handle/2250/138810>. 2015.
2. ARAVENA LÓPEZ, CHRISTIAN ANDRÉS y DE LA FUENTE GÓMEZ, OLIVER NICOLAS. *Régimen Contractual de las Redes Sociales en Internet*. Santiago, Chile. [Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile]. 2010.
3. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS. *Principios rectores para la reglamentación de los ficheros computarizados de datos personales* [archivo pdf]. Resolución 45/95. 14 de Diciembre de 1990. <http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf> [consulta: 10 de Diciembre de 2021]
4. BAMBROUGH, BILLY., Forbes. *La razón por la que Elon Musk apoya Dogecoin y no Shiba Inu, Bitcoin o Ethereum*. 28 de Octubre de 2021 <https://forbes.es/criptomonedas/122821/la-razon-por-la-que-elon-musk-apoya-dogecoin-y-no-shiba-inu-bitcoin-o-ethereum/> [consulta: 10 de Diciembre de 2021]
5. CABEZAS LOGAN, PATRICIO. y MOYA MUÑOZ, FERNANDO. *El derecho al anonimato del usuario de internet*. Santiago, Chile. [Memoria para optar al grado de Licenciado en Ciencias Jurídicas, Universidad de Chile]. 2008.
6. CÁMARA DE DIPUTADOS DE CHILE. *Evaluación de la Ley N° 19.628. Protección de la Vida Privada*. [archivo pdf]. http://www.evaluaciondelaley.cl/wp-content/uploads/2019/07/informe_final_ley_19628_con_portada.pdf [consulta: 10 de Diciembre de 2021]
7. CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (18 de Diciembre de 2000) [archivo pdf]. https://www.europarl.europa.eu/charter/pdf/text_es.pdf [consulta: 10 de Diciembre de 2021]
8. CASADO RIERA, CARLA. (2017). *Personalidad y preferencias de uso en las redes sociales en línea* [archivo en pdf]. Universitat Ramon Llull. FPCEEB - Psicología. Barcelona. <http://hdl.handle.net/10803/409670> [consulta: 10 de Diciembre de 2021].
9. CERDA SILVA, ALBERTO. *Legislación sobre protección de las personas frente al tratamiento de datos personales*. Centro de Estudios en Derecho Informático. Santiago. 2012.

10. CERRILO, CELIA. Occam. *Ejemplos y estrategias del neuromarketing*. 17 de Mayo de 2021
<https://www.occamagenciadigital.com/blog/ejemplos-y-estrategias-del-neuromarketing> [consulta: 10 de Diciembre de 2021]
11. CONSEJO DIRECTIVO DEL CONSEJO PARA LA TRANSPARENCIA (31 de agosto de 2011) *Recomendaciones del consejo para la transparencia sobre protección de datos personales por parte de los órganos de la administración del Estado* [archivo pdf]. <https://www.consejotransparencia.cl/wp-content/uploads/2020/01/RECOMENDACIONES-Para-organismos-del-Estado.pdf> [consulta: 10 de Diciembre de 2021]
12. COLOMER, JAVIER. HSN Blog. *Nootrópicos para Potenciar la Inteligencia*. 16 de Enero de 2020
<https://www.hsnstore.com/blog/suplementos/concentracion-memoria/nootropicos/> [consulta: 10 de Diciembre de 2021]
13. CORNEJO, MARÍA ISABEL. El Mostrador. *Neuroderechos y neurotecnologías en Chile: Prioridades legislativas*. 26 de Julio de 2021
<https://www.elmostrador.cl/noticias/opinion/columnas/2021/07/26/neuroderechos-y-neurotecnologias-en-chile-prioridades-legislativas/> [consulta: 10 de Diciembre de 2021]
14. CHAHUÁN, FRANCISCO, COLOMA, JAIME, DE URRESTI, ALFONSO., GIRARDI, GUIDO., GOIC, CAROLINA. Proyecto de Ley Boletín N° 13828-19. *Sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías* [en segundo trámite constitucional]. 7 de octubre de 2020
<https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=14385&prmBOLETIN=13828-19> [consulta: 10 de Diciembre de 2021]
15. CYBERCLICK. *Marketing Directo. ¿Qué es el marketing directo? Ventajas y ejemplos*.
<https://www.cyberclick.es/marketing/marketing-directo> [consulta: 10 de Diciembre de 2021]
16. DAVARA, MIGUEL ANGEL. *De las autopistas de la información a la sociedad virtual*. Pamplona, Editorial Aranzadi S.A. 1996.
17. DEL FIERRO ACEVEDO, CAMILO. *Derecho al olvido ante los servicios de búsqueda en internet*. Santiago, Chile.[Memoria para optar al grado de Licenciado en Ciencias Jurídicas, Universidad de Chile]. 2018.
18. DEMETRIO CRESPO, EDUARDO. *Fragmentos sobre neurociencias y derecho penal*. Buenos Aires, Argentina. Editorial B de F. 2017
19. DIEZ-PICAZO, LUIS. y GULLON, ANTONIO. *Sistema de Derecho Civil*. (Vol. II). Tecnos. 1989.
20. EFE. Cotizalia. *El dogecoin cae un 30% después de que Elon Musk bromee con que "es un timo"* . 10 de Mayo de 2021

https://www.elconfidencial.com/mercados/2021-05-10/dogecoin-caida-elon-musk-programa_3072099/ [consulta: 10 de Diciembre de 2021]

21. El Economista América.com. (29 de agosto de 2016). *El Economista América*. <https://www.eleconomistaamerica.cl/telecomunicacion-tecnologia-cl/noticias/7790793/08/16/Redes-sociales-los-limites-de-lo-publico-y-lo-privado.html> [consulta: 13 de Octubre de 2021].
22. ESTEVE GONZALEZ, LYDIA. *Aspectos Internacionales de las infracciones de derechos de autor en Internet*. Editorial Comares. España. 2006.
23. FACEBOOK. (22 de octubre de 2020). *Condiciones de Servicio*. <https://es-es.facebook.com/legal/terms> [consulta: 10 de Octubre de 2021]
24. JARAMILLO, OSCAR. (2010). *La desarticulación de lo público y lo privado en las redes sociales* [archivo pdf]. Las audiencias activas, nuevas formas de participación pública. Consideraciones éticas y jurídicas, ISBN 970996206X [consulta: 8 de Octubre de 2021].
25. JERVIS ORTIZ, PAULA. *La Regulación del Mercado de Datos Personales en Chile*. [Tesis para optar al grado de Magíster en Derecho, Universidad de Chile]. Santiago. 2006.
26. LEON ROBAYO, EDGAR. (Junio, 2006). *La posesión de los bienes inmateriales*. Revista de Derecho Privado núm. 36 [archivo pdf]. Universidad de Los Andes. Bogotá, Colombia. <https://www.redalyc.org/articulo.oa?id=360033184002> [consulta: 2 de Noviembre de 2021].
27. LOPEZ SANTA MARÍA, JORGE. *Los Contratos Parte General*. (2º ed., Vol. 1). Santiago. Editorial Jurídica de Chile. 1998.
28. MAYER-SCHÖNBERGER, VIKTOR. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton: Princeton University Press. 2009.
29. MIKE BLAKE. RT. *Neuralink apunta al cerebro humano: Elon Musk anuncia pruebas para incrustar microchips neuronales en personas en 2022*. 8 de Diciembre de 2021 <https://actualidad.rt.com/actualidad/412955-elon-musk-anuncia-pruebas-humanos-neuralink> [consulta: 10 de Diciembre de 2021]
30. MURILLO DE LA CUEVA, PABLO LUCAS. *Informática y Protección de Datos Personales*. Cuadernos y Debates Nº43. Centro de Estudios Constitucionales. Madrid, España. 1993.
31. NACIONES UNIDAS (1948). *Declaración Universal de Derechos Humanos*. <https://www.un.org/es/about-us/universal-declaration-of-human-rights> [consulta: 10 de Diciembre de 2021]

32. NAVAS NAVARRO, SUSANA. (01 de marzo de 2015). *La personalidad virtual del usuario de internet* [archivo en pdf]. Centro de Estudios de Consumo. Universidad Autónoma de Barcelona, Madrid. <https://blog.uclm.es/cesco/files/2015/03/La-personalidad-virtual-del-usuario-de-internet-.pdf> [consulta: 1 de Diciembre de 2021].
33. NIEVA FENOLL, JORDI. *La ciencia jurisdiccional, novedad y tradición. Proceso y Derecho*. Madrid, España. Ed. Marcial Pons. 2016.
34. PÉREZ LUÑO, ANTONIO ENRIQUE. *La Tercera Generación de Derechos Humanos*. Aranzadi. 2006.
35. OSBORNE CLARKE. *Internet de las cosas y propiedad sobre la información*. <https://www.osborneclarke.com/es/insights/internet-de-la-cosas-y-propiedad-sobre-la-informacion> [consulta: 10 de Diciembre de 2021]
36. RESOLUCIÓN DE MADRID. (2010) *Estándares Internacionales sobre Protección de Datos Personales y Privacidad* [archivo pdf]. https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf [consulta: 10 de Diciembre de 2021]
37. SUÑÉ LLINÁS, EMILIO. *Tratado de Derecho Informático*. Volumen I: Introducción y Protección de Datos Personales. Universidad Complutense Madrid, España. 2000.
38. TABLADO, FERNANDO, Grupo Atico 34 (8 de Enero de 2020) *Guía sobre la privacidad digital*. https://protecciondatos-lopd.com/empresas/privacidad-digital/#Que_es_la_privacidad_digital [consulta: 10 de Diciembre de 2021].
39. TERWAGNE, CÉCILE DE. (2012). *Privacidad en Internet y el derecho a ser olvidado/derecho al olvido* [archivo pdf]. Revista de Internet, Derecho y Política. http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-terwagne_esp/n13-terwagne_esp [consulta: 8 de Diciembre de 2021]
40. TWITTER. (19 de Agosto de 2021). *Términos y condiciones de servicio*. <https://twitter.com/es/tos> [consulta 8 de Noviembre de 2021]
41. UNIVERSITAT DE BARCELONA. Departamento de Psicología Social y Psicología Cuantitativa. http://www.ub.edu/psicologia_ambiental/introduccion [consulta: 26 de Octubre de 2021]
42. VERGARA, MANUEL. *Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales* [archivo en pdf]. (Vol. 6, Número 2). Universidad de Chile, Santiago. <https://doi.org/10.5354/0719-2584.2017.45822> [consulta: 3 de Diciembre de 2021].
43. VIOLLIER, PABLO. (Febrero de 2017) *El Estado de la protección de datos personales en Chile* [archivo pdf], Ed. Derechos Digitales.

<https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf> [consulta: 10 de Diciembre de 2021]

44. VISION INTEGRAL, en: <https://visionintegral.org/> [consulta: 10 de Diciembre de 2021]

Leyes.

1. Boletín N°11.144. Proyecto de ley, iniciado en mensaje de S. E. Presidenta de la República. *Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales*. 2007.
2. Boletín N° 13.828-19. Proyecto de ley, iniciado en moción de los Honorables Senadores señor Girardi, señora Goic, y señores Chahuán, Coloma y De Urresti. *Sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías*.
3. Código Civil de Chile. Biblioteca del Congreso Nacional de Chile. Última versión 18 de Noviembre de 2021.
4. Constitución Política de la República. Biblioteca del Congreso Nacional de Chile. 22 de Septiembre de 2005. Última versión 25 de Octubre de 2021
5. Cuaderno de trabajo N° 13 (2019). Democracia y Protección de Datos Personales en la Era Digital. Consejo para la transparencia.
6. Dictamen N° 6.696. *Uso de cuentas personales y bloqueo de usuarios*. (23 de marzo de 2020). Contraloría General de la República de Chile.
7. Dictamen N° 14.953. *Hernández Olmedo, Luis., con Ministro de Relaciones Exteriores*. (4 de julio de 2019). Contraloría General de la República de Chile.
8. Dictamen N° 18.671. *Lobos G., Manuel y Zuñiga Vera., David con la Policía de Investigaciones de Chile*. (10 de julio de 2019). Contraloría General de la República de Chile.
9. Dictamen N° 43.233. *Fernández., Gene por Estatutos de Carabineros de Chile, feriados y uso de tecnologías*. (1 de julio de 2015). Contraloría General de la República de Chile.
10. Ley N° 19.628 Sobre Protección de la Vida Privada. Biblioteca del Congreso Nacional de Chile. 28 de Agosto de 1999. Última versión 26 de Agosto de 2020
11. Ley N° 20.285 Sobre Acceso a la Información Pública. Biblioteca del Congreso Nacional de Chile. 20 de Agosto de 2008. Última versión 1 de Marzo de 2020