



UNIVERSIDAD DE CHILE
FACULTAD DE DERECHO
DEPARTAMENTO DE DERECHO PROCESAL

**PROTECCIÓN DE DATOS PERSONALES EN LA
APLICACIÓN DE TELEFONIA MÓVIL WHATSAPP
MESSENGER**

**MEMORIA DE PRUEBA PARA OPTAR AL GRADO DE
LICENCIADO EN CIENCIAS JURIDICAS Y SOCIALES**

AUTOR

IGNACIO ANDRÉS MOLINA RAMÍREZ

PROFESOR GUÍA

DANIEL ÁLVAREZ VALENZUELA

Santiago de Chile

2015

TABLA DE CONTENIDO

	Página
Introducción.....	1

Capítulo I

Derecho a la Vida Privada

1.1 Origen Histórico del derecho a la vida privada.....	5
1.2 Tres importantes conceptos en el derecho a la vida privada.....	11
1.2.1 Privacidad.....	12
1.2.2 Vida privada.....	13
1.2.3 Intimidad.....	17
1.3 El concepto de derecho a la vida privada.....	19
1.3.1 Conceptos unitarios.....	19
1.3.2 Conceptos multidimensionales.....	25
1.3.3 Derecho a la vida privada como un concepto de configuración gradual...	28
1.3.4 Las posiciones negativas.....	29
1.3.5 La gran deuda de nuestra doctrina.....	31
1.3.6 Más allá de un concepto de vida privada.....	32
1.3.6.1 Las categorías de sistematización de Solove.....	34

Capítulo II

Telefonía Móvil

2.1 Aspectos Generales.....	38
2.1.1 ¿Qué es la telefonía móvil?.....	38
2.1.2 Como funciona.....	39
2.1.3 Los teléfonos celulares.....	43
2.2 Evolución de la telefonía móvil.....	44
2.2.1 Historia de la telefonía móvil.....	44
2.2.2 La comunicación móvil.....	47
2.2.3 Primera generación de teléfonos móviles.....	48
2.2.4 Segunda generación de teléfonos móviles.....	49
2.2.4.1 Transferencia de datos en 2G.....	51
2.2.4.1.1 GSM.....	52
2.2.4.1.2 GPRS.....	52
2.2.4.1.3 EDGE.....	53
2.2.5 Tercera generación de teléfonos móviles (3G).....	54
2.2.5.1 Transferencia de datos en 3G.....	55
2.2.5.1.1 UMTS.....	55
2.2.5.1.2 EV-DO.....	56
2.2.6 Cuarta generación de teléfonos móviles (4G).....	56
2.3 Sistema operativo móvil.....	58
2.3.1 ¿Qué es un sistema operativo?.....	58
2.3.2 Sistemas operativos más utilizados en el mundo.....	61
2.4 Internet móvil.....	65
2.4.1 Internet.....	65
2.4.2 ¿Qué es internet móvil?.....	66
2.4.3 El dilema de la transferencia de datos.....	68

Capítulo III
Privacidad y Telefonía Móvil

3.1 El riesgo de Hansel y Gretel.....	70
3.2 El Riesgo a la privacidad.....	72

Capítulo IV
Protección de Datos Personales en Chile

4.1 Historia de la protección de datos personales en Chile.....	75
4.1.1 Anteproyectos de ley elaborados durante el régimen militar.....	76
4.1.2 Proyectos de ley respecto a la protección de datos personales.....	78
elaborados luego de 1990	
4.2 Aspectos generales de la protección de datos personales en Chile.....	79
4.3 Principios que informan la ley chilena de protección de datos personales.....	80
4.4 ¿Qué es un dato personal?.....	82
4.5 Clasificación de los datos personales.....	85
4.6 Protección constitucional.....	88
4.7 Análisis de la Ley N° 19.628”Sobre protección de la vida privada”.....	90
4.7.1 Generalidades.....	90
4.7.2 Ámbito de aplicación.....	91
4.7.3 Objetivos.....	94
4.7.4 Estructura.....	96
4.7.5 Tipos de datos consagrados.....	98
4.7.6 Requisitos para realizar un tratamiento de datos.....	101
4.7.7 Sujetos que participan en el tratamiento de datos.....	102

6.7.7.1 El titular de los datos.....	102
6.7.7.2 El responsable del registro de banco de datos.....	103
6.7.7.3 Cesionarios.....	104
4.7.8 Derechos de los titulares de datos personales.....	104
4.7.8.1 Derecho de información en la recogida de datos.....	105
4.7.8.2 Derecho de acceso.....	106
4.7.8.3 Derecho de modificación.....	107
4.7.8.4 Derecho de eliminación o cancelación.....	108
4.7.8.5 Derecho de bloqueo.....	110
4.7.8.6 Derecho a conocer la comunicación de datos.....	112
4.7.8.7 Derecho de oposición.....	112
4.7.8.8 Derecho de indemnización.....	113
4.7.9 Obligaciones del responsable del tratamiento de datos personales.....	114
4.7.10 Acciones que contempla la ley.....	115
4.7.11 Habeas Data en la Ley N° 19.628.....	116
4.7.11.1 Causales de procedencia.....	117
4.7.11.2 Legitimación activa y pasiva.....	119
4.7.11.3 Tribunal competente para conocer del Habeas Data.....	119
4.7.11.4 Tramitación.....	120
4.7.11.4.1 Procedimiento ordinario.....	121
4.7.11.4.2 Procedimiento especial.....	124
4.7.12 Principales críticas a la Ley N° 19.628.....	127

Capítulo V

Android, las .app y WhatsApp

5.1 Android, el sistema operativo que cambio la historia de la telefonía.....	132
5.2 Las .app.....	133
5.3 Android, aplicaciones y privacidad.....	135

5.4 WhatsApp Messenger.....	139
5.4.1 ¿Cómo funciona WhatsApp Messenger?.....	141
5.4.2 Seguridad en WhatsApp Messenger.....	143
5.4.3 Términos de servicio.....	146
5.4.4 Política de privacidad.....	157
5.4.5 Constitución de California y el derecho a la privacidad.....	168
5.4.6 California Online Privacy Protection Act.....	168

Capítulo VI

GSMA

6.1 GSMA: La Asociación Profesional Global de la Industria Móvil.....	173
6.2 Móviles y privacidad.....	174
6.3 Cuales son los datos personales según la GSMA.....	175
6.4 Directrices respecto al almacenamiento de datos y privacidad.....	176
Conclusiones.....	181
Bibliografía.....	188

RESUMEN

La presente memoria tiene por objeto analizar la importancia de la aplicación de telefonía móvil WhatsApp Messenger sobre el derecho a la vida privada y la protección de datos personales. Para ello, en el primer capítulo, se analizará qué se entiende por derecho a la vida privada, su contenido, y las teorías más relevantes que pretenden intentar explicar el ámbito de aplicación de este derecho. En el segundo capítulo, explicaremos qué es la telefonía móvil, sus inicios, cómo funciona, su evolución y las principales tecnologías al respecto. Además, nos referiremos a internet móvil, y cómo influye esta tecnología en la telefonía celular. En el tercer capítulo, introduciremos la discusión de cómo influye en la privacidad el vertiginoso avance de la tecnología móvil, principalmente al riesgo que podría conllevar a la privacidad de las personas. En el cuarto capítulo, se analizará el marco normativo de la protección de datos personales en nuestro país, comparando la evolución que ha tenido desde los primeros intentos de regular esta materia, hasta el principal cuerpo normativo existente y su aplicación hoy. El quinto capítulo, tratará principalmente sobre la aplicación de telefonía móvil WhatsApp Messenger, saber qué es, cómo funciona, sus términos de servicios y políticas de privacidad, y su impacto en la privacidad de sus usuarios. El sexto y último capítulo, se referirá a la principal asociación profesional global de la industria móvil (GSMA), y cuál es su postura respecto al impacto que ha significado la telefonía móvil en nuestra privacidad, para esto explicaremos cuales son los datos

personales para la GSMA y las directrices que ellos manejan para el almacenamiento de estos datos y su privacidad.

INTRODUCCIÓN

Día a día el mundo cambia a nuestro alrededor, por una parte esto se debe al ciclo natural de la tierra, y por otro, a la intervención de la mano y mente del hombre. Sin duda, podríamos hablar hoy de una segunda era dorada después de la ilustración, una que ha sido marcada por los avances y desarrollos tecnológicos.

Cuestiones que veíamos e imaginábamos solo en libros y películas, hoy se han vuelto realidad gracias al avance conjunto que han ido desarrollando las distintas ciencias en general. Basta ver como los profesionales químicos han descubierto las bondades del litio para retener electricidad, y aplicar esta capacidad en casi todos los aparatos electrónicos de nuestro tiempo.

En un mundo tan globalizado como el de hoy, en donde rápidamente el desarrollo de las tecnologías rompen cada vez más las barreras físicas de la distancia, la telefonía celular se ha erguido como uno de los avances más significativos del último tiempo. Su crecimiento ha sido exponencial en la última década, y el teléfono celular ha pasado de ser un simple aparato de comunicación por voz, a un moderno dispositivo capaz de realizar las más variadas tareas que las personas se propongan. En ello también ha contribuido el avance del internet, específicamente con el internet móvil y las redes de tercera y cuarta generación, las llamadas redes 3G y 4G.

Nuestro sistema normativo estructurado básicamente en códigos de siglos pasados, ha tenido que saber prever y asimilar los numerosos cambios que en la sociedad conlleva el dinámico crecimiento tecnológico. Crecimiento que en general, adelanta en años a los proyectos y normativas de regulación de la materia, y en las que en poco tiempo, ya han tenido que ser modificadas o derogadas para acompañar al incesante avance de la tecnología. Al final, debemos conformarnos muchas veces con aplicar la normativa existente a estos nuevos conflictos, careciendo de una ley precisa y efectiva al respecto.

Los hombres de ley, sin embargo, en la incansable tarea de regulación normativa ante el dinamismo social, siempre han podido encontrar en la Constitución Política de la República respuestas ante el vacío legislativo, lo que ha permitido de alguna manera, convertir a nuestro máximo cuerpo normativo, en una luz ante la oscuridad que muchas veces se nos presenta.

La historia de la telefonía móvil no tiene más de cincuenta años de vida, el primer “Smartphone” o “teléfono inteligente” fue lanzado al mercado el año 1994, el IBM Simon, que fue el primer teléfono que unía una pantalla táctil, un sistema operativo y las primeras aplicaciones o programas de celular, lo que convertían al teléfono en algo más que un medio para comunicarse. En 1997, la empresa Ericsson crea lo que oficialmente se consideraría el primer “Smartphone” o “teléfono inteligente”, el Ericsson GS88, que incluía dentro de sus aplicaciones el primer navegador de internet, toda una revolución en la tecnología celular.

Hoy en día, a no más de veinte años del IBM Simon, los teléfonos móviles han alcanzado un nivel muy avanzado respecto de sus predecesores, transformándose en pequeños computadores portátiles. Lo anterior permitió la creación de ejecutables en un celular, las llamadas “aplicaciones”, que actualmente permiten al usuario llevar a cabo casi cualquier tarea en ellos, más aún, cuando cualquier persona con un grado avanzado de conocimiento de programación, puede desarrollar sus propias aplicaciones móviles y compartirlas con los demás gratuitamente.

“WhatsApp Messenger” es una de estas aplicaciones para teléfonos inteligentes, que permite básicamente la comunicación SMS, similar a un chat, entre dos o más personas. La aplicación nos permite enviar imágenes, sonidos y videos desde un celular a otro, todo de una manera rápida y expedita, con la única necesidad de poseer una conexión a internet.

WhatsApp Messenger fue creada en el año 2009, y en tan solo dos años ya contaba con más de 100 millones de clientes en todo el mundo, un verdadero éxito tecnológico que significó un gran cambio en la comunicación social.

La realidad es que el avance de la telefonía inteligente, ha significado que las personas vean sus expectativas de privacidad fuertemente disminuidas, y lo anterior muchas veces, sin siquiera el sujeto darse cuenta de ello. A lo anterior se nos presenta la siguiente pregunta ¿cuánto cuesta tu privacidad? la respuesta es que muy poco para saber quién eres, ¿a qué hora te despiertas y te acuestas?, ¿dónde vas a trabajar?, ¿dónde vas a vacacionar?, ¿quiénes son tus padres?, ¿quién es tu esposa(o) y tus hijos?, y ¿qué haces día a día en tu vida?. Entonces la verdadera pregunta que cabe

hacernos es ¿cuánto estas dispuesto a sacrificar de tu privacidad por una mejor tecnología?

El derecho ha intentado regular esta materia, y ha buscado las formas de proteger tu vida privada. El dilema, es que la tecnología siempre ha estado por delante del derecho, y la normativa muchas veces no avanza lo suficientemente rápido para regular estos cambios. En este sentido, analizaremos la Ley N° 19.628 “*Sobre Protección de la Vida Privada*”, que a pesar de su nombre, sólo se dedica a regular la protección de datos de carácter personal. De todas maneras, veremos cómo aplicar esta normativa, y qué es lo que realmente protege de nuestra privacidad al utilizar aplicaciones como WhatsApp.

Seguramente en unos pocos años más, todo esto será historia y estaremos hablando por ejemplo de telefonía holográfica 3D, teléfonos del tamaño de una moneda o móviles que funcionaran directamente insertados a nuestro sistema nervioso, etcétera. Sin mayores dudas, a pesar de todo esto, nuestra normativa no estará mucho más adelantada de lo que hoy se encuentra, y tendremos los mismos problemas al intentar aplicar leyes que no están destinadas específicamente a estos dilemas. Es nuestro deseo, poder ayudar a entender mejor la protección de los datos personales en la telefonía móvil de última generación, más específicamente, frente a nuevas aplicaciones como la que en este trabajo analizaremos.

CAPITULO I

DERECHO A LA VIDA PRIVADA

1.1 Origen histórico del derecho a la vida privada

El derecho a la vida privada¹ como tal, surge en los EE.UU. en el año 1890, a propósito del caso Warren y Brandeis. La señora de Samuel Warren (un próspero y reconocido abogado de Estados Unidos) llevaba una vida social muy activa en Boston y en su hogar recibía a personas importantes del estado de Massachusetts. Los diarios locales se empeñaban en obtener hasta los más mínimos detalles de lo que ocurría al interior de la casa de la familia Warren, a fin de poder publicarlos. Cuando la hija de los Warren se casó, las intromisiones e informaciones de la prensa fueron más insolentes que nunca. Es entonces que el Sr. Warren preocupado de los límites a la privacidad, decide contactarse con su socio Luis Brandeis (quien más tarde se convertiría en uno de los más grandes jueces de la *Supreme Court* durante

¹ Para Tom Gerety, el derecho a la vida privada se traduce en la privacidad de las personas, la que debe ser comprendida como la “autonomía o control sobre las intimidades de la identidad personal”. Señala que la forma paradigmática de invasión de la vida privada es la injerencia sobre la autonomía sexual. Este modo de concebir el derecho a la vida privada y la lucha ideológica en contra de las reglas tradicionales que han reglamentado los comportamientos en el plano de la sexualidad, es realmente llamativa: tanto que se ha dicho que el abuelo del derecho a la privacidad, más que Warren y Brandeis, parece haber sido Freud, pues, es la concepción freudiana de la personalidad la que coloca a la sexualidad en un lugar privilegiado de la formación de nuestra identidad. CORRAL TALCIANI, HERNÁN. 2000. Configuración Jurídica del Derecho a la Privacidad II: Concepto y Delimitación. [en línea] Revista Chilena de Derecho, Vol. 27 N°2, p.331-355, Sección Estudios. 2000. <<https://corraltalciani.files.wordpress.com/2010/04/configuracion-juridica-del-derecho-ii.pdf>> [consulta: 22 enero 2015]

25 años²) con el objeto de escribir y publicar en la revista de la Facultad de Derecho de la Universidad de Harvard, su estudio sobre el derecho a la intimidad titulado *The Right of Privacy*. Así, en el año 1890, Warren y Brandeis sostuvieron que ya era hora de que se reconociera el derecho a la intimidad y propusieron las reglas generales en la materia y los límites del derecho. Para lo anterior, suministraron diversos ejemplos de atentados a la vida privada, especialmente de aquellos cometidos por la prensa, expresando así la atención sobre el interés que tienen los individuos en la tranquilidad del hogar y en la exclusiva reserva de las informaciones concernientes a sus actividades personales³.

La privacidad por estos autores fue concebida de la noción que poco antes desarrollara el juez norteamericano Cooley, proclamado el “derecho de ser dejado tranquilo y de no ser arrastrado a la publicidad”, como lo propio del derecho a la intimidad⁴.

En nuestro país, el profesor Eduardo Novoa Monreal, señala que inicialmente la jurisprudencia norteamericana rechaza el concepto de vida privada. Sin embargo, esta comienza a reconocerlo en forma gradual, pero con formas y fundamentos divergentes de las que hoy son más generalmente aceptadas. Solamente en el caso

² WARREN, SAMUEL. y BRANDEIS, LOUIS. 1995. El derecho a la intimidad. Madrid, Civitas. p.17

³ EDITORIAL JURIDICA DE CHILE. 1982. Revista de derecho y jurisprudencia y gaceta de los tribunales. [en línea] Santiago de Chile, Editorial Jurídica de Chile. <<http://books.google.cl/books?id=J1I2rgulunAC&printsec=frontcover#v=onepage&q&f=false>> [consulta: 01 diciembre 2014]

⁴ NOVOA MONRREAL, EDUARDO. 1997. Derecho a la vida privada y la libertad de información: Un conflicto de derechos. 5ª ed., Santiago de Chile, siglo veintiuno editores. p.26

*Griswold v. Connecticut*⁵, viene a admitir la Corte Suprema Federal el fundamento constitucional de este derecho⁶.

Con más del doble de historia que EE.UU., países como Francia ya mostraban en su doctrina y jurisprudencia un adelanto importante en la creación jurídica del concepto. Señala Novoa Monreal que hasta antes de la vigencia de la ley del 17 de julio de 1970, que tiene una parte destinada a la “protección de la vida privada”, la doctrina y la jurisprudencia de Francia habían adelantado bastante en la creación jurídica del concepto. Juristas franceses elaboraron primero la noción de los “derechos de la personalidad”, para que luego los tribunales impusieran su respeto por la vía de la aplicación del artículo 1382 del código civil francés, sobre responsabilidad extracontractual. La jurisprudencia al comienzo muy variable, se fue uniformando dentro de un apreciable número de sentencias correspondientes, principalmente, a reclamos de artistas y gente de mundo para asegurar un amplio

⁵ *Griswold v. Connecticut* (1965), es un caso histórico en los Estados Unidos, en el que la Corte Suprema de este país, determinó que la Constitución protege un derecho a la privacidad. Este caso tiene su fundamento en la ley de Connecticut aprobada en 1879, la cual prohíbe el uso de cualquier droga, artículo medicinal, o instrumento con el fin de evitar la concepción. Estelle Griswold (directora ejecutiva de la Planned Parenthood League of Connecticut) y el Dr. C. Lee Buxton (un médico y profesor de la Escuela de Medicina de Yale), abrieron una clínica de control de natalidad en New Haven, Connecticut. Poco después Griswold y Buxton fueron arrestados, juzgados, declarados culpables y obligados a pagar una multa. La condena fue apelada y confirmada por la Corte de Apelaciones y Suprema del estado de Connecticut. Griswold apeló su condena ante el Tribunal Supremo de los Estados Unidos, argumentando que la ley contra el uso de métodos anticonceptivos era contraria a la Decimocuarta Enmienda de la Constitución de Estados Unidos sección primera, según el cual “ningún Estado podrá dictar ni dar efecto a cualquier ley que limite los privilegios o inmunidades de los ciudadanos de los Estados Unidos, ni podrá Estado alguno privar a cualquier persona de la vida, la libertad o la propiedad sin el debido proceso de ley...ni negar a cualquier persona la igual protección de las leyes”. La Corte Suprema de los Estados Unidos llegó a la conclusión de que la ley de Connecticut era inconstitucional, y reconoció el derecho a la privacidad de los matrimonios, en cuanto a decidir usar o no un método anticonceptivo dentro de su vida sexual. Con el tiempo, la Corte Suprema amplió este derecho, específicamente en el caso *Eisenstadt v. Baird* (1972), pues otorgar este derecho a la privacidad solo a las parejas en matrimonio, era una “discriminación irracional”. WIKIPEDIA. *Griswold v. Connecticut*. [en línea] <http://en.wikipedia.org/wiki/Griswold_v._Connecticut> [consulta: 03 noviembre 1998]

⁶ NOVOA MONREAL, EDUARDO. “Derecho a la vida privada y la libertad de información: Un conflicto de derechos”. op. cit., p.26

respeto a la vida privada⁷. Sin embargo, como podemos ver, tanto en este país, como Italia y Alemania, se acercaban más este concepto a lo que se denominaría un derecho de la personalidad⁸. Así, el derecho a la vida privada gozaría de un reconocimiento parcial solo en la medida en que este se encuentre vinculado con el anterior derecho. Incluso en países como Alemania, donde durante mucho tiempo se discutió la existencia del derecho de la personalidad, la Ley Fundamental de 1949, es especial el artículo 1, concede las directrices para que los tribunales de ese país apliquen el derecho a la vida privada como parte de los derechos de la personalidad⁹, y de conceder indemnización por daño moral en caso de desconocimiento de ellos.

En Italia antes de la dictación de la ley del 8 de abril de 1974 (que modificó los códigos penales y de procedimiento penal para incorporar tipos nuevos que amparan el secreto de las comunicaciones de dicha vida privada¹⁰), el reconocimiento de este derecho no era tan claro. La Corte de Casación había negado reiteradamente un derecho a ese secreto por falta de texto expreso que así lo reconociera, no obstante aceptaba que una divulgación de información sobre la vida privada violaría un derecho a la personalidad, protegido en el artículo 2 de la constitución.

⁷ *Ibíd.*, p.26-27

⁸ “El Derecho, por lo tanto, está siempre relacionado a las personas, y el verdadero motivo de su existencia en cuanto rama del conocimiento es exactamente la necesidad de regulación de las relaciones humanas.

(...) Por lo tanto, en cuanto a los derechos de la personalidad, se puede decir que: son aquellos que se refieren a la facultades jurídicas cuyo objeto son los diversos aspectos de la propia persona del sujeto, bien como sus emanaciones y prolongaciones, son todos aquellos destinados a dar contenido a la personalidad, son manifestaciones parciales de la personalidad humana, son condiciones esenciales a su ser y devenir, son aquellos que atienden a manifestaciones de las personalidades en sí mismas.” DRUMMOND, VÍCTOR. 2004. *Internet, Privacidad y Datos personales*. Madrid, España, editorial Reus S.A., p.32-35

⁹ CABEZAS, LOGAN. y MOYA, FERNANDO. 2008. *El derecho al anonimato del usuario de internet*. Memoria de prueba para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile, Facultad de Derecho. [en línea] <http://www.tesis.uchile.cl/tesis/uchile/2008/cabezas_p/html/index-frames.html> [consulta: 15 diciembre 2014]

¹⁰ NOVOA MONREAL, EDUARDO. “Derecho a la vida privada y la libertad de información: Un conflicto de derechos”. *op. cit.*, p.27

Hasta principios del siglo XX, las declaraciones de derechos humanos y las constituciones políticas no hacían referencia específica al derecho al respeto de la vida privada. Sin embargo, en el derecho común de todos los países, podían encontrarse al menos preceptos que prestaban amparo a varios importantes aspectos de ese derecho de manera indirecta a través de otros derechos, como las reglas relativas a la protección de domicilio o de protección de la correspondencia.

En el plano internacional, la Declaración Universal de Derechos Humanos de 1948 en su artículo 12¹¹, reconoce y postula el concepto de “arbitrariedad” entendida como una intervención ilegítima, elemento del cual la vida privada se debe proteger.

El inciso primero del artículo 8 de la Convención Europea de los Derechos del Hombre, reconoce a la persona un derecho a la vida privada.

A nivel regional, la Convención Americana sobre Derechos Humanos de 1969 en San José de Costa Rica, también protege el derecho a la vida privada, reconociéndolo dentro del derecho a la dignidad de la persona en su artículo 11¹².

Los organismos de las Naciones Unidas no se ocupan del derecho a la vida privada sino hasta el 19 de diciembre de 1968, donde se adopta la resolución número

¹¹ 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. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

¹² Protección de la Honra y de la Dignidad

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

2450 (XXIII), en la que se pide al secretario general de la ONU, preparar un informe sobre el respeto a la vida privada de los individuos y la integridad y soberanía de las naciones ante los progresos de las técnicas de registro y de otra índole. Sin embargo, esta petición se funda en la Conferencia Internacional sobre Derechos Humanos, celebrada en Teherán poco tiempo atrás. En dicha conferencia figura una referencia implícita al derecho a la vida privada y se preocupa de las amenazas que constituyen los últimos descubrimientos científicos y adelantos tecnológicos en contra de este derecho y de otros derechos humanos¹³. Desde 1955 organismos no gubernamentales y estudios privados se ocupan de profundizar los aspectos jurídicos de la protección de la vida privada. En este sentido se celebran distintas conferencias, siendo la más importante la celebrada en Estocolmo, los días 22 y 23 de mayo de 1967, llamada Conferencia de Juristas Nórdicos. La UNESCO también llevo a cabo una reunión de expertos sobre derecho a la vida privada en París en enero de 1970.

De esta manera, podemos observar que a través de la historia, en la búsqueda de la creación de un sistema normativo moderno, se ha venido a resolver paulatinamente la preocupación por establecer y garantizar el derecho a la vida privada. Sin embargo, debido a la época en la cual estos y otros documentos han sido redactados, se ha hecho referencia solo a los asuntos derivados de correspondencia, papeles u otros documentos materiales. Por lo tanto, las referencias explícitas a la

¹³ Sorprende al mundo, en esa época, los adelantos tecnológicos en materia de espionaje, entendiendo el momento político vivido, cual es, *La Guerra Fría*. O de las escuchas telefónicas, una novedad practicada desde antes de la segunda guerra mundial. En ese tiempo, la interceptación telefónica se realizaba mediante una derivación, la cual requería empalmar un auricular con los cables telefónicos, en cualquier parte de su curso. Esto permitía al que actuaba escuchar lo que hablaban ambas partes a través del hilo. NOVOA MONREAL, EDUARDO. "Derecho a la vida privada y la libertad de información: Un conflicto de derechos". op. cit., p.99

vida privada en el ámbito digital, que es a lo que a este trabajo le interesa, solo las encontraremos en las legislaciones y trabajos más modernos.

En nuestro país, la referencia normativa al derecho a la vida privada se encuentra en el artículo 19 n°4 de la Constitución Política de la Republica¹⁴.

Además, en lo que a este trabajo se refiere, su protección se encuentra determinada por otras leyes, las cuales serán analizadas en su momento.

1.2 Tres importantes conceptos en el derecho a la vida privada

Precisar y entender claramente el concepto de vida privada es vital para el desarrollo de esta investigación. Puede parecer irrelevante a simple vista la necesidad de poder definir qué se entiende por vida privada, sin embargo, lo que puede parecerse un asunto trivial, ha generado sendas discusiones en el mundo entero¹⁵.

Cuando hablamos de vida privada, el primer problema que se nos presenta es la facilidad con que comúnmente tendemos a confundir los conceptos de privacidad, intimidad y vida privada como si fueran lo mismo. Este error es más común de lo

¹⁴ La Constitución asegura a todas las personas: 4°. El respeto y protección a la vida privada y a la honra de la persona y su familia.

¹⁵ SUAREZ CROTHERS, CHRISTIAN. 2000. El concepto de derecho a la vida privada en el derecho anglosajón y europeo. [en línea] <http://mingaonline.uach.cl/scielo.php?script=sci_arttext&pid=S0718-09502000000100010&lng=es&nrm=iso p.103-120> [consulta: 15 diciembre 2014] p.103-120

que parece, pues, cada una de estas palabras está relacionada una con la otra. Sin embargo, la utilización de una u otra, puede llevarnos a distintas interpretaciones, y al final del día a la hora de aplicar la ley, interpretaciones distintas pueden llevarnos a diferentes decisiones.

1.2.1 Privacidad

El termino privacidad es un anglicismo importado del termino *privacy* utilizado de modo corriente por los Estados Unidos¹⁶. La institución del *privacy* agrupa una serie de derechos subjetivos aceptados por la Corte Suprema Federal y por las Cortes y la legislación de casi todos los Estados Unidos. Ámbitos como la vida familiar, las emociones y la sexualidad son zonas típicas del *privacy*. Según dice Rigaux, PRIVACY significa autonomía o poder (...) aquella esfera de decisiones que el individuo debe poder tomar sin riesgo de la injerencia externa. Incluye el derecho de estar y de permanecer solo (...) Las zonas del PRIVACY son zonas de apropiación cuyo contenido es afectivo, intelectual, religioso y que el sujeto debe poder manejar si quiere permanecer libre (...) La esencia del derecho al PRIVACY consiste en el ejercicio de un derecho de apropiación que impida toda agresión externa, privada o pública¹⁷.

¹⁶ DRUMMOND, VÍCTOR. “Internet, Privacidad y Datos personales”. op. cit., p.31

¹⁷ EDITORIAL JURIDICA DE CHILE. “Revista de derecho y jurisprudencia y gaceta de los tribunales”. op. cit., p.71

Privacidad sería aquello que una persona lleva a cabo en un ámbito reservado, como la vida familiar, relaciones de amistad o la sexualidad, teniendo la persona el derecho a la privacidad y a mantener esta fuera del alcance de otras personas.

La privacidad sería el fundamento de la vida privada, pues, para tener vida privada debe existir privacidad, sin embargo, y en definitiva, privacidad y vida privada son conceptos utilizados con idéntico sentido.

1.2.2 Vida Privada

El profesor Eduardo Novoa Monreal, señala que no existiría un concepto único de vida privada, que se trataría de algo relativo y, por consiguiente, variable conforme a ciertas condiciones. *La idea que se tiene de la vida privada varía “de una persona a otra, de un grupo a otro, de una sociedad a otra; varía también igualmente, en función de edades, tradiciones y culturas diferentes”*¹⁸.

Sin embargo, a pesar de lo variable y relativo que pueda ser el concepto, el profesor Novoa Monreal explica que pueden existir diversas actividades, situaciones y fenómenos que pueden a la luz de la doctrina, declararse pertenecientes a la vida privada, reconociendo una cantidad considerable de ellas, pero que en un análisis minucioso, cada una de ellas puede ser agrupadas de acuerdo a ciertas características

¹⁸ NOVOA MONREAL, EDUARDO. “Derecho a la vida privada y la libertad de información: Un conflicto de derechos”. op. cit., p.42

comunes que se repiten como una constante, ya sea en forma explícita o implícita. Estas características son¹⁹:

- a. *que se trata de manifestaciones o fenómenos que normalmente quedan sustraídos al conocimiento de personas extrañas o cuando menos ajenas al círculo familiar del sujeto, o de sucesos que no se desarrollan normalmente a la vista de dichas personas;*
- b. *que los hechos referidos son de aquellos cuyo conocimiento por otros provoca normalmente al sujeto una turbación moral en razón de ver afectado su sentido del pudor o del recato;*
- c. *que el sujeto no quiere que otros tomen conocimiento de esos hechos.*

Es así como Novoa Monreal logra, sobre la base de estas características comunes, intentar una definición general de la vida privada, señalando: “*que la vida privada está constituida por aquellos fenómenos, comportamientos, datos y situaciones de una persona que normalmente están sustraídos al conocimiento de extraños y cuyo conocimiento por éstos puede turbarla moralmente por afectar su pudor o su recato, a menos que esa misma persona asienta a ese conocimiento*”²⁰. Es decir, es todo lo cual se quiere mantener fuera del conocimiento público (lo que cualquier persona puede conocer ejercitando los más mínimos derechos que su sistema normativo les

¹⁹ NOVOA MONREAL, EDUARDO. “Derecho a la vida privada y la libertad de información: Un conflicto de derechos”. op. cit., p.45-49

²⁰ NOVOA MONREAL, EDUARDO. “Derecho a la vida privada y la libertad de información: Un conflicto de derechos”. op. cit., p.49

otorgue²¹). De lo anterior, se hace necesario identificar algunos otros conceptos claves para comprender mejor la definición que el profesor Novoa nos entrega. Primeramente está el carácter no conocido de los hechos, específicamente por estar *sustraídos al conocimiento de extraños*. Por extraños debe entenderse a todas las personas que no constituyen el grupo familiar más próximo y a los parientes que participan en la parte más íntima de la vida. No quiere decir esto que solo los hechos que tengan lugar dentro del hogar pertenezcan a la vida privada (por ser el hogar el ambiente familiar más próximo), sino que además, hay muchos hechos y situaciones de nuestra vida que tienen lugar en oficinas, hogares de amigos o conocidos y otros recintos cerrados, que están también dentro de ellos. Además, en esta definición se recoge la importancia de la voluntad del sujeto para delimitar que en su vida puede considerarse como parte de la esfera pública o privada²². Y es en este sentido donde se plantea uno de los más grandes problemas que se suscitan al respecto, la de determinar si los hechos que se desarrollan en lugares públicos o abiertos pueden considerarse como parte de la vida privada.

En la discusión de la comisión Ortúzar se expresó por parte del señor Ovalle: “que es más conveniente la expresión vida privada en vez de la palabra privacidad porque el concepto de vida privada está más desarrollado en el lenguaje común. Ya hay una especie de reconocimiento en la colectividad de que lo que se respeta es la vida privada. No es la vida hacia el exterior; es la vida interna, dentro del hogar; y la

²¹ CABEZAS, LOGAN. y MOYA, FERNANDO. “El derecho al anonimato del usuario de internet”. op. cit., p.14

²² “De manera obvia son titulares del derecho a la vida privada todos los seres humanos, dentro de lo que su cultura y su medio tengan por vida privada. También los incapaces son titulares, si bien no pueden ejercerlo, sino con asistencia de su representante legal”. En relación a lo determinante de la voluntad en el sujeto en poder decidir sobre el ejercicio del derecho a la vida privada. Así la incapacidad no permite ejercer este derecho sino a través de un representante legal. NOVOA MONREAL, EDUARDO. “Derecho a la vida privada y la libertad de información: Un conflicto de derechos”. op. cit., p.59

privacidad es un término menos usado, menos conocido. En cambio, la forma vida privada, constituye una referencia más permanente.

Asimismo, considera preferible la alternativa b) porque las constituciones y las declaraciones de derechos, en general, no hablan de privacidad, sino de algo más concreto, que forma parte de la privacidad, que es la vida privada; la vida familiar o la vida personal, y no la vida pública, la vida externa, que si puede ser discutida. Puede decirse, por ejemplo: Tal abogado intervino en una defensa... Esa no es su vida privada, sino su vida hacia el exterior”²³.

El derecho a la privacidad no se encuentra recogido como tal por nuestra legislación, pero, a nuestro entender la privacidad sería el fundamento del concepto vida privada, que si se encuentra expresamente normado en nuestra legislación (art. 19 N° 4 y 5 de la Constitución Política de la Republica²⁴). La privacidad como un concepto amplio mueve a la vida privada, la privacidad se protege y es reconocido en nuestra legislación en el derecho a la vida privada, que muchas veces utiliza estos términos como sinónimos.

También, muy relacionado con la vida privada está el concepto de intimidad que veremos a continuación.

²³ BIBLIOTECA DEL CONGRESO NACIONAL. Actas oficiales de la comisión constituyente. [en línea] <http://www.bcn.cl/xbcn3x/lc/cpolitica/constitucion_politica/Actas_comision_ortuzar/Tomo_IV_Comision_Ortuzar.pdf> [consulta: 15 diciembre 2014] p.343-344

²⁴ Esto será tratado en mayor profundidad en el capítulo IV.

1.2.3 Intimidad

El profesor Humberto Nogueira nos señala: *“La vida privada en un círculo o ámbito más profundo lleva al concepto de intimidad. La intimidad es el ámbito reservado del individuo que no desea ser develado al conocimiento y acción de los demás, el cual aparece como necesario para mantener un mínimo de calidad de vida humana. El derecho a la intimidad es la facultad de la persona para evitar las injerencias de terceros en el ámbito de su privacidad, salvo autorización de tal develamiento de la intimidad por el propio afectado.”*²⁵

A pesar de que hay autores en nuestro sistema doctrinal chileno que tienden a utilizar como sinónimos los conceptos de intimidad y vida privada²⁶, creemos, y así lo hemos dado a entender al comienzo de este capítulo, que estos dos conceptos, como el concepto de privacidad, no son sinónimos. Lo anterior es compartido por el profesor Nogueira Alcalá, en la distinción que acabamos de analizar.

La diferencia fundamental entre intimidad y vida privada radica en el hecho de que la intimidad entiende aspectos más sensibles de la vida privada, es solo una parte de ella. Involucra las creencias de la persona, y aquellos hechos que este ha

²⁵ NOGUEIRA ALCALÁ, HUMBERTO. 2002. El derecho a la libertad de opinión e información y sus límites: honra y vida privada. Santiago de Chile, Universidad de Talca y Lexis Nexis. p.174

²⁶ Novoa Monreal señala que no se advierte la necesidad de hacer una diferenciación entre lo privado y lo íntimo. En la misma línea, José Luis Cea señala que la vida privada busca asegurar el Derecho a la Intimidad. CABEZAS, LOGAN. y MOYA, FERNANDO. “El derecho al anonimato del usuario de internet”. op. cit., p.16

decidido mantener en secreto para sí o para su entorno más inmediato, sean familiares o parientes cercanos.

En la discusión de la comisión Ortúzar se expresó por parte del señor Guzmán “es importante –y así se ha dicho en sesiones anteriores de la Comisión- destacar la introducción de dos valores distintos de la inviolabilidad del hogar y de la correspondencia en forma tradicional que se consagraba, y que son los que el señor Silva Bascuñán en su proposición procura establecer a través de los términos respeto a la intimidad y al honor de las personas. Piensa sin embargo, que el primer concepto se expresa en forma más adecuada y completa en la noción de privacidad, porque ésta envuelve el ámbito de una zona de la vida privada de la persona que debe quedar precisamente excluida de la noticia de la invasión externa.

La intimidad, continua, es todavía una zona más profunda y sensible que la privacidad. Es algo todavía más sutil y, por lo tanto, de menos alcance en su extensión”²⁷.

Como conclusión podemos señalar que la “vida privada”, contiene los aspectos más sensibles de la vida de una persona, aspectos que no se quieren que sean conocidos. “El derecho de vida privada se viola en el momento en que un extraño – entendemos por tal para este efecto a cualquiera, salvo a aquellos que en razón de cierta clase de relaciones íntimas o de la aceptación de su titular sean partícipes del secreto – toma conocimiento de cualquier parte de aquello que hemos indicado como el ámbito de la vida privada”²⁸. Es decir, basta que un extraño penetre

²⁷ BIBLIOTECA DEL CONGRESO NACIONAL. “Actas oficiales de la comisión constituyente”. op. cit., p.335

²⁸ NOVOA MONREAL, EDUARDO. “Derecho a la vida privada y la libertad de información: Un conflicto de derechos”. op. cit., p.58

en ella y tome conocimiento de lo reservado sin ser necesario que la divulgue y, que su revelación provoque un daño en la persona que va ligado a otros derechos de la esencia del ser humano.

1.3 El concepto de derecho a la vida privada²⁹

Son muchas las formulaciones que se han hecho al respecto, y la tarea de intentar lograr dar efectivamente con la esencia de este derecho, se hace inabordable por la cantidad de literatura existente en el tema³⁰. Sin embargo, en base al análisis hecho por Corral Talciani, nos referiremos a aquellas formulaciones que nos parecen más relevantes a la hora de intentar dar con este concepto. Para esto, Corral divide el análisis entre aquellos conceptos unitarios, multidimensionales, de configuración gradual y de posiciones negativas del derecho a la vida privada.

1.3.1 Conceptos unitarios

a) El derecho a ser dejado solo

²⁹ CORRAL TALCIANI, HÉRNAN. “Configuración Jurídica del Derecho a la Privacidad II: Concepto y Delimitación”. op. cit., p.331-355

³⁰ FIGUEROA, RODOLFO. 2013. El derecho a la privacidad en la jurisdicción de protección. Revista Chilena de Derecho, 40 (3): 859-889

La famosa frase del juez Cooley citada por el trabajo de Warren y Brandeis, viene a sostener que la esencia del derecho a la vida privada reside en este “ser dejado solo” o “ser dejado en paz” o “no ser molestado” (lo que podemos llamar *seclusión*³¹ o tranquilidad), según las distintas versiones que en español puede ser traducida la frase “*the right to be let alone*”.

Esta frase es muy utilizada por los jueces de la Corte Suprema norteamericana para conceptualizar el derecho a la vida privada. Sin embargo, su utilización para explicitar la noción del derecho a la vida privada no es adecuada, pues, un sujeto puede sufrir interferencias que le impiden ser dejado solo o no ser molestado de mil maneras, y muchas de ellas nada tienen que ver con lo que queremos ordinariamente significar con la idea de privacidad. Así, por ejemplo, golpear a otro estaría dentro de este derecho a “ser dejado en paz”, pero nadie podría decir que aquí existiría una invasión a la vida privada.

De esta forma la conceptualización del derecho a la vida privada falla por su tremenda amplitud, que puede llevar a una inflación de los supuestos hechos protegidos por la intimidad, y confundir en vez de aclarar su función específica.

³¹ Del inglés *seclusion* que se traduce como aislarse, alejarse de la comunidad. Barros utiliza este anglicismo. BARROS, ENRIQUE. 1998. Honra, privacidad e información: un crucial conflicto de bienes jurídicos. Revista de Derecho, Universidad Católica del Norte, año 5: 45-58.

b) El derecho a tomar decisiones personales

Fue la Corte Suprema norteamericana la que señaló que el derecho a la vida privada, en última instancia, significaba el derecho a adoptar libre de injerencias ajenas decisiones que afectaran directamente la vida personal. Es la línea de razonamiento que se vislumbra en el caso Griswold (1965), que se afirma en el caso Eisenstadt (1972) y se ratifica en Roe (1973).

Esta concepción, ha sido seriamente cuestionada por no aportar criterios objetivos para determinar cuándo una decisión personal debe ser libre de trabas e injerencias y cuándo en cambio esa decisión debe ser reprobada y desalentada. Además, cuando se conceptualiza privacidad como autonomía se genera una confusión con el concepto de libertad.

c) El derecho al control de la información personal

La privacidad consistiría en el control que cada persona puede ejercer sobre la información que le concierne. En Chile, Enrique Barros adhiere a esta posición.

La dificultad de conceptual de definir el derecho a la privacidad como el control de la información, lleva a la conclusión de que si la persona se expone al público debe señalarse que está perdiendo privacidad ya que pierde control sobre la información que otros están adquiriendo de ella. Por otro lado, si una persona decide voluntariamente dar a conocer un hecho personal a otra, estará ejerciendo su poder de control pero al mismo tiempo estará perdiendo privacidad.

Sobre lo anterior, Parent de manera muy lucida señala que “El control sobre la información personal no es una condición necesaria de privacidad, si por ‘control’ queremos significar el poder de prevenir la revelación de tal información a otros individuos que a aquellos que hemos elegido para revelarla. Supóngase que B tiene las destrezas tecnológicas y la autoridad política para obtener toda suerte de información personal acerca del ciudadano A. Y aún supongamos que A nada puede hacer para detener a B de hacerlo y de revelar los hechos conocidos a cualquiera que él quiera. Bajo estas circunstancias A carece de control sobre estos hechos: él no tiene poder para prevenir la revelación que hace B. Pero ¿ha perdido A su privacidad? No, no a menos que B actualmente proceda a iniciar una acción de intromisión y diseminación en contra suya. Que A tenga amenazada su privacidad no significa que ella le haya sido disminuida”³².

³² CORRAL TALCIANI, HÉRNAN. “Configuración Jurídica del Derecho a la Privacidad II: Concepto y Delimitación”. op. cit., p.333-334

d) El derecho a la inaccesibilidad

Esta tesis viene a mejorar la propuesta del control de la información personal. Sin embargo, cae en la misma imposibilidad que critica Parent a la del control de la información.

e) El derecho a excluir a terceros de la información personal

Se postula la idea de que la privacidad no debe ser entendida en un sentido positivo como “control” o “inaccesibilidad” o “autonomía”, sino más bien, como la facultad negativa de exclusión en un cierto tipo de información acerca de la persona.

Parent en este sentido acuña el siguiente concepto de privacidad: la condición de que otros no conozcan información personal acerca de uno mismo que no haya sido documentada.

Esta definición de Parent, se critica en el hecho de que el concepto de información personal que se propone, es más bien normativo, careciendo del intento de describir fácticamente el contenido de la privacidad. Además, se aduce que esta postura no se pronuncia sobre un

aspecto esencial y es qué información puede o debe estar en registros públicos.

Otra crítica aún más incisiva, que se dirige a la doctrina de la “información no documentada”, es que deja fuera todos los casos en los que terceros invaden el ámbito privado pero no adquieren nuevo conocimiento sobre el sujeto afectado.

f) El derecho sobre el acceso cognoscitivo

Esta definición es propuesta por Madison Powers, que sostiene que una definición de privacidad debe ser descriptiva, y por lo tanto no contaminarse con elementos normativos que son más propios del análisis posterior sobre la extensión o limitación de un derecho a la vida privada.

Critica las tesis de la privacidad como autonomía, control o inaccesibilidad, que él denomina como “antirreduccionistas”, por su vaguedad e imprecisión.

Básicamente esta teoría viene a señalar que, todas las conductas que lleven a una persona a tomar conocimiento sobre hechos personales de otra resultan contrarias a la vida privada. Corral es de la idea que esta

definición, aunque restringida, resulta funcional para elaborar una aproximación coherente sobre el conjunto de los derechos de las personas, pues, de muchos tipos de interferencias una persona puede experimentar múltiples pérdidas, incluyendo la libertad (a través de la compulsión), privacidad (a través de un incrementado acceso cognoscitivo), integridad física (a través de un incrementado acceso sobre el cuerpo) y la soledad (a través de un incrementado acceso a la proximidad física)³³.

Se puede oponer a esta posición que no considera los casos en que el conocimiento no se obtiene de manera directa, sino que indirecto a través de la difusión de lo que se conoció por la injerencia indebida en la intimidad de la persona afectada.

1.3.2 Conceptos multidimensionales

a) Noción cuatripartita

³³ CORRAL TALCIANI, HÉRNAN. “Configuración Jurídica del Derecho a la Privacidad II: Concepto y Delimitación”. op. cit., p.336

Es una de las nociones multidimensionales más importantes en el derecho angloamericano, que ha sido propuesta por uno de los más grandes expertos en el campo de *torts*³⁴, William L. Prosser.

El estudio de Prosser es netamente jurisprudencial. Consiste en ordenar y descubrir que es lo que los tribunales, en su país, han entendido por *privacy*. Luego de examinar cerca de trescientos casos judiciales sobre el derecho a la vida privada, propone que no puede hablarse de un solo ilícito o *tort* a ella, sino de un complejo de cuatro *torts*, que comprenden cuatro tipos de invasión a cuatro diferentes intereses de la víctima. Estos *torts* son: 1) intrusión en el retiro (seclusión) o soledad de la víctima, o en sus asuntos privados; 2) Revelación pública de hechos embarazosos acerca de la víctima; 3) Publicidad que coloca a la víctima en una imagen falsa ante los ojos del público, y 4) Apropiación, para provecho del demandado, de nombre o de la apariencia de la víctima.

La posición de Prosser ha sido muy importante, y permanece como una herramienta útil para clasificar los distintos objetos del derecho a la privacidad en el campo de los daños civiles.

Esta propuesta de Prosser, ha sido fuertemente criticada, pues, se ha equivocado al disgregar el significado de la vida privada otorgando diferentes contenidos y finalidades a la figura, ya que, existe un elemento común en todas ellas, y que permite identificar cuando la privacidad está siendo violada, que es la pérdida de dignidad.

³⁴ Del inglés *Tort*, que se traduce al español, en este caso, como Ilícito.

Corral señala que esta crítica no es persuasiva. Que la intención de Prosser no era más que describir. De un modo sistemático y relativamente coherente, el estado jurisprudencial del concepto de privacidad, y no asumir una posición normativa intentando buscar cuál es el interés general que ampara el Derecho al reconocer la vida privada como objeto de protección³⁵.

b) Noción tripartita

Estas nociones buscan caracterizar la esencia del derecho a la privacidad identificando sus modos operativos en tres funciones. Algunos autores que desarrollan esta teoría son Judit DeCew y Rut Gavison, que señalan que la privacidad envuelve tres aspectos relevantes para conceptualizarla como tal.

c) Noción bipartita

La noción bipartita podemos encontrarla en la doctrina francesa de Kayser, y de acuerdo a la posición de este autor, la vida privada

³⁵ CORRAL TALCIANI, HÉRNAN. “Configuración Jurídica del Derecho a la Privacidad II: Concepto y Delimitación”. op. cit., p.338

contempla dos posibles facetas: el *secret du la vie privée* (incluye la exclusión del conocimiento de aspectos de la vida personal y familiar) y *la liberté de la vie privée* (dice relación con el poder de conducir la vida privada del modo que parezca más conveniente).

1.3.3 Derecho a la vida privada como un concepto de configuración gradual

Ante el hecho absoluto de que toda persona tiende a resguardar con mayor o menor precaución ciertos tipos de información, se ha formulado la teoría alemana de las esferas (*Sphärentheorie*).

Según esta tesis existirían tres tipos de esferas: la esfera íntima o del secreto (*Geheimsphäre*), con el más alto grado de protección; la esfera privada (*Vertrauensphäre*), que comprende los comportamientos, noticias y expresiones que el sujeto no desea que se conozcan públicamente; y la esfera social (*Privatsphäre*), que comprendería todo aquello que no se encuentra dentro de las anteriores dos esferas y que tendría el menor grado de protección.

Esta teoría ha sido criticada en cuanto a la dificultad que supone una definición exacta de las distintas esferas, pues, estas son difíciles

de diferenciar y, además, para las distintas personas pueden tener un distinto contenido.

En Chile, defiende esta teoría de las esferas el profesor Cea Egaña. El hace la diferencia entre dos tipos de esferas, en primer lugar la esfera de la intimidad, que se refiere a los datos sensibles, específicamente a la manera de ser de cada uno, sus actitudes o gustos, lo más secreto de su conciencia o de su físico. Por otro lado estaría la esfera de la privacidad, que dice relación con aquellas informaciones que no son tan sensibles, pero que siguen siendo hechos o circunstancias que su titular desea mantener bajo reserva³⁶.

1.3.4 Las posiciones negativas

Dentro de las posiciones negativas encontramos aquellas teorías que de una u otra manera abandonan la idea de ofrecer un concepto claro y preciso de la privacidad. En este sentido, encontramos a Raymon Wack, que sostiene que el debate por tratar de fijar un concepto de privacidad es estéril y fútil. Es estéril porque toda

³⁶ La Corte de Apelaciones de Puerto Montt en sentencia de 18 de marzo de 1997, resolviendo un recurso de protección relativo a informaciones comerciales (DICOM), se pronuncia sobre el derecho a la vida privada, y distingue entre la *esfera íntima* que solo corresponde a cada persona en particular y que el sujeto no está dispuesto a compartir con nadie y la *esfera de la vida privada* que sí se puede compartir con determinadas personas. La distinción para la Corte no tienen ninguna importancia para el caso que se resuelve. C.A. de Pto. Montt, 18 de marzo de 1997, RDJ t. 94, sec. 5ª, p. 193.

definición es hecha desde perspectivas de análisis diferentes, no parten de los mismos materiales ni de los mismos objetivos, lo que impide establecer un concepto como más acertado que otro. Es fútil porque cuando en un sistema los tribunales o la ley hablan de privacidad, privacidad será lo que ellos digan.

Otros piensan, señala Corral, que todo lo que no sea vida pública pertenecerá a su vida privada.

Finalmente están otro que prefieren una enumeración no taxativa de aspectos, hechos o circunstancias que compondrían la vida privada. Lindon, ex fiscal del Tribunal Supremo francés y pionero del derecho de la prensa³⁷, en respuesta a la teoría de definir vida privada como todo aquello que no es vida pública, criticándola por la imprecisión de los términos extremos, establece que existen ciertos elementos significativos de la vida privada que podemos distinguir y que es donde existe privacidad, estos elementos son: a) la vida familiar; b) la vida amorosa; c) la imagen; d) los recursos y los impuestos que paga y; e) el tiempo libre.

³⁷ DIARIO EL PAÍS. 1992. Raymond Lindon, pionero del derecho de Prensa. [en línea] El País Archivo. 30 de enero, 1992. <http://elpais.com/diario/1992/01/30/agenda/696726001_850215.html> [consulta: 22 de enero 2015]

1.3.5 La gran deuda de nuestra doctrina

A pesar de que hoy en día existe una mayor preocupación por establecer que podemos entender por vida privada, aún la tarea no está completa. Una rápida revisión de la jurisprudencia de nuestros tribunales superiores de justicia, nos permite ver como nuestros tribunales no se encargan de definir lo que se entiende como vida privada, sin embargo, establecen dimensiones o ámbitos donde podemos entender que hay vida privada. Por ejemplo encontramos el caso Alvarado Solari contra Diario *la Cuarta*³⁸, en donde la Corte establece como elemento determinante de la vida privada, el espacio físico donde se realiza o tiene lugar cierto hecho o circunstancia para determinar si se ha violado o no el derecho a la vida privada³⁹. Encontramos también situaciones en que la Corte incluso se ha atrevido a entregar una definición de vida privada. Es el caso Martorell con Chile, donde se definió “vida privada” como aquella zona que el titular del derecho no quiere que sea conocida por terceros sin su consentimiento, así también se definió vida pública como aquella que llevan los hombres públicos y de la que conocen terceros, aun, sin su consentimiento, siempre que sean de real trascendencia⁴⁰.

³⁸ C.A. Santiago, 1 de agosto de 1989, diciembre-marzo 1990, p. 126 y sgtes.

³⁹ El actor interpone recurso de protección en favor de su hija, la cual es fotografiada en una playa del litoral, y cuya fotografía es incluida por el diario La Cuarta, en dos ediciones (en la portada), sin que haya habido autorización ni menos conocimiento de parte de la afectada. El tribunal resolviendo el presente recurso, señala que no podría existir una afectación al derecho a la vida privada, pues, las fotografías son tomadas a una bañista que se encuentra en una playa, esto es, en un lugar público, lo cual “está indicando que la presunta afectada no lo considera privado”.

⁴⁰ Sentencia caso Martorell. Rol N° 983-93, 15.06.1993. Revista de Derecho y Jurisprudencia, Tomo XC (2), sección 5

A pesar del gran esfuerzo que ha hecho nuestra doctrina y jurisprudencia por intentar dar con un concepto definitivo de vida privada, la tarea aún persiste, más aún cuando nuestra extensa literatura esta al debe en cuanto a sistematizar las categorías o ámbitos que estarían comprendidos por el derecho a la privacidad, cuestión relevante para poder definir el contenido de lo que comprende el derecho a la vida privada⁴¹. Tampoco, nuestra literatura se ha dedicado a sistematizar la jurisprudencia producida con ocasión de este derecho, salvo cuatro importantes autores que se han dado a esta tarea⁴², por lo demás, existe una importante deuda a este respecto.

1.3.6 Más allá de un concepto de vida privada

Como podemos ver, la tarea por establecer un concepto de vida privada es extremadamente complejo. Señalar una definición inequívoca al respecto, es prácticamente imposible. Sin embargo, en este sentido, un trabajo que merece destacarse es el elaborado por Corral Talciani, (el cual además nos ha permitido desarrollar de manera estructurante estos capítulos), que define privacidad como bien jurídico en los siguientes términos: *“es la posición de una persona (o entidad colectiva personal) en virtud de la cual se encuentra libre de intromisiones o difusiones cognoscitivas de hechos que pertenecen a su interioridad corporal o*

⁴¹ Es el autor anglosajón Solove, quien ha realizado uno de las grandes categorizaciones o ámbitos que estarían comprendidas en el derecho a la privacidad. Este autor distingue cuatro dimensiones de la privacidad, las que contienen un total de 16 categorías de privacidad, que es mucho más de lo que ha identificado la doctrina chilena. En nuestro país se han hallado casos para 13 de estas 16 categorías que propone Solove.

⁴² Pedro Anguita; Gastón Gómez; María Rodríguez y; Mauricio Tapia. FIGUEROA, RODOLFO. “El Derecho a la Privacidad en la Jurisdicción de Protección”. op. cit., p.859-889.

psicológica o a las relaciones que ella mantiene o ha mantenido con otros, por parte de agentes externos que, sobre la base de una valoración media razonable, son ajenos al contenido y finalidad de dicha interioridad o relaciones”⁴³.

Corral sin duda hizo una magnífica labor al definir la privacidad, aportando significativamente con la deuda de nuestra literatura por entender este concepto, por entender en definitiva este derecho. Es arriesgada la tarea de establecer una sola definición de privacidad o vida privada, porque los tribunales vienen aplicando distintas nociones al respecto en la resolución de cada caso que es puesto en su conocimiento. Si nos diéramos a la labor de sistematizar la jurisprudencia en base a una sola noción, como por ejemplo, a la dada por Corral, nos veríamos en la dificultad de identificar privacidad en cada caso en particular, lo que produciría cierta distorsión en la sistematización. Por tanto, nos parece mucho más acertado, establecer, como lo hace Solove, categorías que permitan entender cuando hay privacidad, y cuando esta debe ser protegida.

Establecer categorías de sistematización jurisprudencial escapa a los objetivos de este trabajo, sin embargo, la importancia de conocerlos, nos permitirá entender mejor manera cuando hay un derecho a la privacidad. Para lo anterior mencionaremos brevemente las categorías establecidas por Solove, ya que, este autor ha identificado muchas más de lo que lo ha hecho nuestra doctrina chilena.

⁴³ CORRAL TALCIANI, HÉRNAN. “Configuración Jurídica del Derecho a la Privacidad II: Concepto y Delimitación”. op. cit., p.338

1.3.6.1 Las categorías de sistematización de Solove⁴⁴

Solove reconoce cuatro dimensiones con dieciséis categorías en total, que son las siguientes:

I. Recolección de información

Esta dimensión consiste en la captación de información. Comprende dos categorías: Vigilancia (en esta categoría, la privacidad se ve afectada por actos de vigilancia sobre la persona) e; Interrogación (en esta categoría, la privacidad se vulnera cuando una persona es sometida a un interrogatorio que le exige revelar datos sobre sí mismo).

II. Procesamiento de información

Esta dimensión consiste en el uso, almacenamiento y manipulación de información que ha sido recolectada. Comprende cinco

⁴⁴ FIGUEROA, RODOLFO. “El Derecho a la Privacidad en la Jurisdicción de Protección”. op. cit., p.863 -883

categorías: Agregación consiste en conectar diversas partes aisladas de información para construir un perfil identificable de una persona); Identificación (Consiste en conectar información que existe en alguna base de datos o registro con una persona en particular); Inseguridad (esta categoría se refiere al temor que el titular tiene acerca de la protección que recaiga sobre información suya almacenada en alguna base de datos); Uso secundario (consiste en emplear información privada para un fin distinto de aquel para el cual fue obtenida); Exclusión (consiste esta categoría en la facultad del titular de poder acceder a, corregir y/o eliminar información personal que exista en algún registro o base de datos).

III. Diseminación de Información

Esta dimensión de privacidad, consiste, en general, en la divulgación de información privada, y es la que normalmente produce mayor daño a este derecho. Comprende siete categorías de divulgación: Quiebre de confidencialidad (consiste en la revelación de información privada por parte de quien la recibió bajo secreto profesional); Revelación (consiste en revelar o divulgar a terceros información privada verdadera de una persona); Exposición (consiste en mostrar el cuerpo de una persona contra su voluntad, sin su autorización, en términos tales que la avergüence, humille o denigre); Accesibilidad

aumentada (aumentar el acceso a terceros de información privada que tiene un grado reducido de publicidad); Chantaje (consiste en amenazar a alguien con la revelación de información privada del sujeto); Apropiación (consiste en la utilización de la imagen o identidad de un tercero para fines propios); Distorsión (consiste en diseminar cierto tipo de información o hacerlo de cierto modo que conduce a equívoco y afecta la manera como los demás ven o perciben a una persona).

IV. Invasión⁴⁵

Cuarta y última dimensión, comprende dos categorías: Intrusión (que consiste en entrometerse en la soledad o reclusión de un individuo o en sus asuntos privados) e; Interferencia Decisional (interferencia del gobierno en las decisiones de las personas relativas a ciertas materias de su vida).

La sistematización de categorías de privacidad es a nuestro juicio mucho más importante que una noción de privacidad, es el principio de donde debería partir todo intento por definir la vida privada, ya que, conocer los fundamentos que estructuran este derecho, en base a un entendimiento acabado de lo que la privacidad en su esencia comprende, permitiría una mejor definición de su concepto, lo que ayudaría

⁴⁵ Esta dimensión de privacidad se distingue de las anteriores en un factor esencial: no implica necesariamente información.

a las cortes resolver de una mejor manera los casos que se le presenten, protegiendo efectivamente y cuando corresponda, toda vulneración a este importante derecho.

CAPITULO II

TELEFONÍA MÓVIL

2.1 Aspectos generales

2.1.1 ¿Qué es la telefonía móvil?

La telefonía móvil, también llamada telefonía celular, es aquella tecnología que permite la comunicación telefónica con un emisor y un receptor que están en movimiento. Este movimiento al cual nos referimos, denota la capacidad en el cual el usuario dispone de un terminal que no es fijo, es decir, permite que aquel puede estar en casi en cualquier lugar y comunicarse con otra en cualquier parte. Esto es posible gracias a que esta tecnología excluye casi por completo la utilización de cables para conectar físicamente los dos extremos de un teléfono, utilizando como medio de transmisión ondas electromagnéticas⁴⁶. Lo anterior permite una serie de beneficios, como una mayor ancho de banda, evitar las amenazas externas a las que son más propensos los cables y, la movilidad y comunicabilidad de los usuarios. Esto se lleva a cabo a través de un aparato llamado Teléfono Móvil o Teléfono Celular,

⁴⁶BARRÍA, SUSANA. 2007. Webmóvil: desarrollo de soporte comunicacional web a través de dispositivos de telefonía móvil [en línea] <http://www.tesis.uchile.cl/tesis/uchile/2007/barria_s/html/index-frames.html> [consulta: 22 enero 2015]

que no es más que un teléfono que funciona de manera similar a una radio de un solo canal. Un teléfono celular utiliza dos frecuencias diferentes: una para hablar y otra para escuchar. Con un teléfono móvil básicamente se puede marcar un número para hacer una llamada o recibir una llamada.

2.1.2 Cómo Funciona⁴⁷

Es un servicio de radio celular que se basa en dar cobertura a un territorio a través de diversas estaciones base. La idea detrás de esta tecnología, es la división de la ciudad en pequeñas células o celdas (de aquí el nombre *telefonía celular*)⁴⁸. Esto permite la re-utilización de frecuencias a través de la ciudad, con lo que miles de personas pueden usar los teléfonos al mismo tiempo, evitando el problema de la restricción del ancho de banda. Cada celda generalmente tiene un tamaño de 26 kilómetros cuadrados y estas son diseñadas como hexágonos (figura de seis lados), para poder abarcar todo el espacio en una gran rejilla de hexágonos. Cada celda tiene una *estación base transmisora* que son unidades fijas controladas por una unidad de control (que es un pequeño edificio que contiene el equipo de radio que controlan de forma automática las emisiones o el funcionamiento de una estación base) que tiene una amplitud para emitir y recibir en ese hexágono. Cada célula utiliza varias decenas de canales, cada canal emite las señales (ondas electromagnéticas) a una frecuencia

⁴⁷AREATECNOLOGIA. Telefonía Móvil. [en línea] <<http://www.areatecnologia.com/telefonía-movil.htm>> [consulta: 22 enero 2015]

⁴⁸BARRÍA, SUSANA. “Webmóvil: desarrollo de soporte comunicacional web a través de dispositivos de telefonía móvil”. op. cit., p. 11

diferente. Esto permite tener múltiples canales para el uso de decenas de celulares de manera simultánea, lógicamente cada una a su frecuencia. Cuando un usuario pasa de una célula a otra deja la frecuencia que estaba utilizando, para el uso de otro celular, y toma la frecuencia libre de la célula a la que pasó⁴⁹.

50

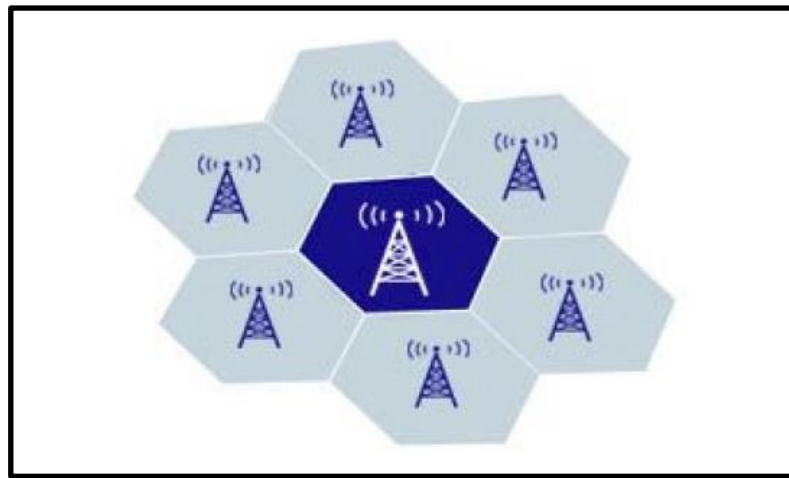


Ilustración 1: Diseño de transmisión de señal celular

Un proveedor de servicio celular típicamente recibe 832 radios frecuencias para utilizar en una ciudad. Cada teléfono celular utiliza dos frecuencias por llamada, por lo que entonces habrían típicamente 395 canales de voz por portador de señal (las 42 frecuencias que sobran serían ocupadas como canales de control). Por lo tanto, cada celda tiene alrededor de 56 canales de voz disponibles. En otras palabras, en cualquier celda, pueden haber 56 personas hablando por sus teléfonos celulares al

⁴⁹ BARRÍA, SUSANA. “Webmóvil: desarrollo de soporte comunicacional web a través de dispositivos de telefonía móvil”. op. cit., p. 11-13

⁵⁰ Imagen tomada del sitio: ZONATRADE. Celulares. [en línea] <<http://www.zonatrade.com/Celulares/Celulares.htm>> [consulta: 22 enero 2015]

mismo tiempo. Esta división en células, hace que los teléfonos celulares necesiten menos energía para transmitir y alcanzar cualquier estación base o antena reemisora que cubre un área más pequeña, reduciendo la energía necesaria para la transmisión, lo que reduce el tamaño de la batería y consecuentemente el peso y el tamaño de los celulares.

Luego de las primeras tecnologías de telefonía celular, que eran análogas, se crea una tecnología mucho más avanzada; la tecnología de transmisión digital móvil. Con la transmisión del sistema digital, el número de canales disponibles aumenta significativamente. Por ejemplo en el sistema digital TDMA⁵¹, que es un sistema digital de segunda generación (2G), se pueden llevar a cabo el triple de llamadas en cada celda, alrededor de 168 canales disponibles simultáneamente. Esto supone a simple vista, una menor utilización de energía de los celulares.

Entonces, cuando una persona utiliza su teléfono celular, lo primero que hace el teléfono es, localizar la estación base con la señal más fuerte que pertenezca a la red de su operador y, solicita un canal. La estación base permitirá el acceso al canal (a menos que no haya más espacio en la celda, situación que puede ocurrir cuando muchas personas ocupan su teléfono celular al mismo tiempo copando los canales⁵²)

⁵¹ Conocido también como Digital AMPS (D-AMPS). Se describe en el estándar internacional IS-54 y en su sucesor IS-136. Hoy esta tecnología ha sido reemplazada en su mayoría por las tecnologías GSM (conocida por ser la tecnología de la generación 2.5) y posteriormente UMTS (Universal Mobile Telecommunications System) sistema digital de tercera generación (3G). Hace algún tiempo se ha comenzado a aplicar también el nuevo estándar LTE (Long Term Evolution) una interfaz radioeléctrica basada en OFDMA (Orthogonal Frequency-Division Multiple Access) que caracteriza a la red de cuarta generación (4G). SLIDESHARE. 2012. Historia de la telefonía celular. [en línea] <<http://www.slideshare.net/javitojr/historia-de-la-telefonía-celular-12598330>> [consulta: 22 enero 2015]

⁵² En Chile situaciones así han ocurrido en los casos de emergencia, donde una gran cantidad de personas utiliza su teléfono celular, saturando los canales en las celdas.

y la llamada es entonces aceptada. La central de conmutación⁵³ de la estación base, deriva (busca) al destinatario deseado (por su número de teléfono móvil receptor), en la red de estaciones bases (celdas) hasta encontrar a la que pertenezca en ese momento y conecta las dos estaciones bases emitiendo una alerta, llamada, al teléfono receptor. Si el receptor acepta la llamada los pone en contacto. La información, en este caso la voz, se transmite por ondas electromagnéticas de una antena a otra. Los comunicantes están conectados por medio de la red de antenas (estaciones bases). Cuando la central de conmutación encuentra la celda a la que pertenece el receptor, la central de conmutación de la estación base a la que pertenece el móvil receptor, da la frecuencia a la que deben operar los dos móviles para comenzar la transmisión. Cuando un móvil entra en una zona de una célula, la estación base lo detecta, lo asigna a esta célula y lo registra. Si la persona se mueve a otra zona, el móvil tomara otra celda diferente. En el caso de no encontrar ninguna célula, el móvil estará fuera de cobertura.

54

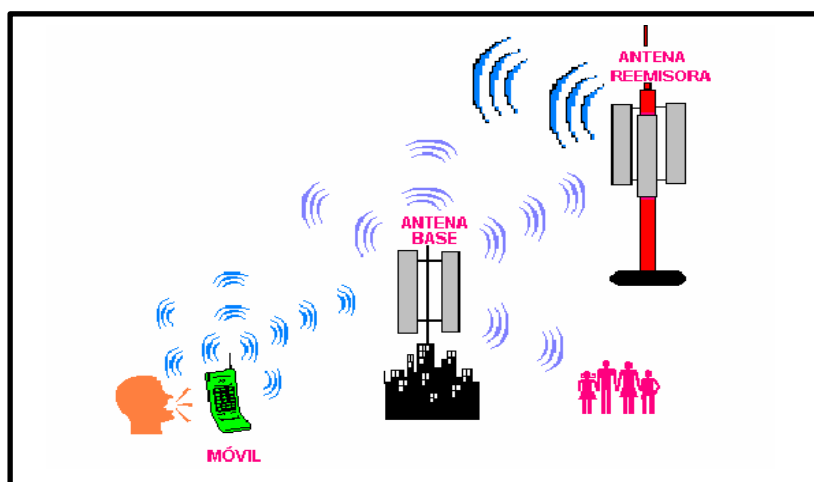


Ilustración 2: Elementos de la señal de transmisión celular

⁵³ Las centrales de conmutación suplantaron a las viejas operadoras que unían dos teléfonos mediante clavijas.

⁵⁴ Imagen tomada del sitio: AREATECNOLOGIA. Telefonía Móvil. [en línea] <<http://www.areatecnologia.com/telefonía-movil.htm>> [consulta: 22 enero 2015]

2.1.3 Los teléfonos celulares⁵⁵

Los celulares son dispositivos electrónicos con diseños complejos e intrincados, con partes encargadas de procesar millones de cálculos por segundo solo para comprimir o descomprimir el flujo de voz. Hoy en día, la complejidad de los teléfonos celulares ha ido aumentando debido a la gran cantidad de funcionalidades que se pueden desarrollar en él. Sin embargo, al desarmar un teléfono celular, a pesar de su mayor o menor tecnología, es posible encontrar una serie de partes comúnmente identificables:

- Una placa de circuito integrado que contiene el cerebro del teléfono.
- Una antena.
- Teclado.
- Pantalla LCD (display de cristal líquido).
- Una Batería.
- Un Micrófono.
- Un Altavoz.
- Una cámara fotográfica (En el caso de los celulares más avanzados)

⁵⁵ QUIMINET. 2011. ¿Cómo funciona el teléfono celular? [en línea] < <http://www.quiminet.com/articulos/como-funciona-el-telefono-celular-2571317.htm> > [consulta: 22 enero 2015]

El chip de la compañía proveedora de telefonía celular⁵⁶ y la memoria (MicroSD comúnmente) son accesorios externos insertables en el teléfono móvil.

2.2 Evolución de la telefonía móvil

2.2.1 Historia de la telefonía móvil

El teléfono fue inventado en 1876 por el científico y logopeda estadounidense de origen escocés, Alexander Graham Bell⁵⁷, y la comunicación inalámbrica tiene sus raíces en la invención del radio por Nikolai Tesla en la década de 1880, aunque formalmente fue presentado en 1894 por un joven italiano llamado Guglielmo Marconi⁵⁸.

Los primeros sistemas de telefonía móvil civil empiezan a desarrollarse a partir de finales de los años 40 en los Estados Unidos. En esta época, la gente que realmente necesitaba comunicación móvil tenía que confiar en el uso de radio-teléfonos instalados en sus autos. En el sistema radio-telefónico, existía solo una antena central por cada ciudad, y probablemente unos 25 canales disponibles en la torre. Esta antena central hacía que el teléfono en el vehículo fuera equipado con una antena

⁵⁶ En nuestro país son compañías proveedoras de servicio móvil: Entel, Movistar, Claro, VTR, Nextel, Virgin Mobile.

⁵⁷BIBLIOGRAFIASYVIDA. Alexander Graham Bell. [en línea] <<http://www.biografiasyvidas.com/biografia/b/bell.htm>> [consulta: 15 diciembre 2014]

⁵⁸RADIOCOMUNICACIONES.NET. Historia de la Telefonía Móvil. [en línea] <<http://www.radiocomunicaciones.net/telefonía-movil.html>> [consulta: 22 enero 2015]

suficientemente poderosa, capaz de transmitir a 50 o 60 kilómetros de distancia. Esto significaba, que no muchas personas podrían usar el radio-teléfono, ya que, no existían suficientes canales para conectar.

El concepto de telefonía móvil como tal, tiene su origen en el año 1947 cuando en los *Bell Labs*, del departamento de pesquisa de AT&T, el único operador norteamericano en ese entonces, los científicos desarrollaron las ideas que permitirían el uso de teléfonos móviles usando “células” que identificaban a un usuario en cualquier punto donde se llevara a cabo la llamada⁵⁹. Por entonces, la idea no era realizable debido a las dificultades en la concesión de espectro de radio por parte de las autoridades de Estados Unidos.

La historia de la telefonía celular puede explicarse de la mano de tres de las más importantes empresas desarrolladoras de telefonía del mundo, hablamos de Ericsson, Motorola y Nokia.

A fines de la década de los 50, la empresa Ericsson una de las tres empresas más importantes del rubro en esa época. Puso en marcha lo que se denominó el primer sistema automático de telefonía móvil, que consistía de manera muy sencilla en una estación base con 2 canales y cinco estaciones móviles, cuyos tamaños eran parecidos al de un armario y sus pesos bordeaba los 40 kgs., los que iban montados sobre un vehículo. Estas redes cubrían apenas radios de 25 a 30 kms. Casi paralelamente, la empresa Nokia entraba en el terreno comenzando sus

⁵⁹ BARRÍA, SUSANA. “Webmóvil: desarrollo de soporte comunicacional web a través de dispositivos de telefonía móvil”. op. cit., p. 11-12

investigaciones en transmisiones de radio. Desde entonces las empresas han entrado en una incansable lucha por alcanzar más y mejores tecnologías. Los años siguientes y hasta nuestros días, estas y otras empresas, han estado dedicados a crear aparatos cada vez más avanzados, pequeños, livianos y capaces de establecer mejores y más rápidas comunicaciones.

Las comunicaciones satelitales, el avance de las redes, la fabricación de microchips proponen para las grandes empresas de telefonía móvil un inmejorable escenario para el desarrollo de su industria, de modo que día a día podemos como son lanzados al mercado un sin número de aparatos más compactos y potentes a una velocidad vertiginosa.

A partir de 1960, los *Bell Labs* y Motorola empezaron a estudiar el concepto e intentaron ponerlo en práctica. Sin embargo, la carrera celular fue vencida por Motorola el día 3 de abril de 1973, gracias a los esfuerzos del doctor Martin Cooper. Para muchos, Cooper es el inventor del primer teléfono celular, y se le considera "el padre de la telefonía celular" al crear el primer radioteléfono en Estados Unidos, mientras era gerente general de Motorola. Se dice que Cooper estando en la esquina de una calle en Manhattan, decidió intentar hacer una llamada personal. Cooper, a través de un prototipo de teléfono celular modelo Dyna-Tac diseñado por él, presionó la tecla para conectar el móvil y el aparato logró conectarse a la red fija a través de una estación base instalada en el tope de un edificio. Es así como realizó la primera llamada a Joel Engel, el responsable del departamento de pesquisas de *Bell Labs*⁶⁰.

⁶⁰ TELEFONOS-MOVILES. Martin Cooper - El Inventor De Los Teléfonos Móviles. [en línea] <<http://www.telefonos-moviles.com/articles/item.asp?ID=24>> [consulta: 06 septiembre 2014]

Sin embargo, no fue hasta 1979 cuando aparecieron los primeros sistemas comerciales en Tokio (Japón) por la compañía NTT⁶¹, y apenas en 1982, la FCC (Federal Communication Commission) aprobó en los Estados Unidos el lanzamiento, por parte de la empresa Ameritech, el primer sistema móvil comercial⁶².

2.2.2 La comunicación móvil

Dentro de lo que se refiere a la tecnología móvil, se reconocen dos tipos de comunicación: la que se lleva a cabo por vía terrestre y, la que se realiza vía satelital. La primera utiliza estaciones instaladas en el espacio terrestre, que se encargan por ejemplo, de monitorear la posición de cada terminal encendido, realizar el cambio de control de una llamada en curso a otra estación, enviar una llamada a un terminal suyo, etcétera. Cada estación tiene un área de cobertura, los que son teóricamente hexágonos regulares o celdas como ya hemos visto anteriormente. La segunda, se realiza vía satélite, es decir, sus estaciones de control se encuentran en satélites fuera del espacio terrestre, aunque su órbita suele ser bastante baja en comparación a la mayoría de los satélites (unos 780 km). Su gran ventaja radica en su capacidad de cobertura mundial en relación a la comunicación móvil terrestre y, su principal desventaja deviene en el alto precio de las llamadas y terminales.

⁶¹ DE BERNARDO, CESAR. y PRIEDE, TIZIANA. Marketing Móvil, una nueva herramienta de Comunicación: Análisis y nuevas perspectivas para el mercado español. [en línea], España, Editorial Netbiblo <<https://books.google.cl/books?id=4nz1NoSYiaUC&pg=PA2&lpg=PA2&dq=historia+de+la+telefon%C3%ADa+m%C3%B3vil+bell+laboratories&source=bl&ots=oPaeTNSvwt&sig=3XjZudF3THXvlp4nZHTYzmpNot0&hl=es&sa=X&ei=zyPIVL6VHNWOsQsgroKgBQ&ved=0CDwQ6AEwBQ#v=onepage&q=historia%20de%20la%20telefon%C3%ADa%20m%C3%B3vil%20bell%20laboratories&f=false>> [consulta: 22 enero 2015]

⁶² RADIOCOMUNICACIONES.NET. op. cit.

La telefonía móvil por comunicación terrestre, ha tenido una rápida evolución a diferencia de la telefonía por vía satelital, esto debido a que la tecnología por comunicación terrestre es más asequible para las personas debido a los bajos costos que su implementación implica. Este sistema de conexión de la telefonía celular se ha ido ampliando y desarrollando, paralelamente con la evolución tecnológica de los teléfonos móviles, cuyo proceso de “evolución” se identifica por generaciones. Hasta el momento se cuentan cuatro generaciones de telefonía móvil terrestre.

2.2.3 Primera generación de teléfonos móviles (1G)

La tecnología 1G o primera generación de redes móviles, hizo su aparición a finales de los años setenta y comienzo de los ochenta del siglo pasado. A estos sistemas se les conocían como *celular*, en inglés, pero luego el término fue reducido a “*cell*” en referencia al método que utilizaba para entregar las señales entre una torre y otra. Esta tecnología se caracterizó por ser analógica y estrictamente para voz, y los dispositivos de esta generación eran relativamente menos pesados y costosos que dispositivos anteriores⁶³. La transmisión entre celdas era muy imprecisa y tampoco tenía buena calidad del sonido, ya que estaban basadas en FDMA⁶⁴ (Frequency Division Multiple Access) y, además, la seguridad en esta generación no existía. La

⁶³ Existían equipos celulares antes del nacimiento de la 1G, pero estos teléfonos móviles se veían restringidos por su limitada movilidad y mal servicio. Estos equipos eran tremendamente pesados, pudiendo llegar a pesar varios kilos, y extremadamente caros.

⁶⁴ Tecnología básica en el servicio analógico de la telefonía celular inalámbrica.

tecnología predominante en 1G es AMPS (Advanced Mobile Phone System⁶⁵), el cual se empleó con mayor fuerza en Estados Unidos⁶⁶.

Con la aparición de la red 1G el mercado de teléfonos celulares creció entre un 30% y 50% anualmente, y el número de suscritos mundiales alcanzó aproximadamente veinte millones para 1990.

2.2.4 Segunda generación de teléfonos móviles (2G)

Desde la creación de los primeros sistemas comerciales analógicos de 1G a finales de la década de los setenta y hasta comienzos de los noventa, se evidenció la necesidad de desarrollar estándares comunes a nivel regional, ya que los sistemas 1G eran desarrollados por empresas privadas como AT&T, Motorola o Ericsson, lo que dificultaba la creación de mercados de mayor volumen de usuarios. Lo anterior significó un proceso de estandarización que se desarrolló primeramente en industrias regionales de países como EE.UU., Europa, Japón, Canadá y Corea del Sur, principalmente, lo que por un lado mejoró la compatibilidad dentro de las regiones pero que seguía manteniendo las diferencias entre ellas. Lo anterior se solucionó a comienzo de los años 90 con la implementación de los sistemas de comunicaciones móviles 2G, que primeramente fijó estándares dentro de la industria de origen y sus

⁶⁵ El Sistema Telefónico Móvil Avanzado es un sistema de telefonía móvil de primera generación desarrollado por los *Bell Labs* (Laboratorios Bell). Se implementó por primera vez en 1982 en Estados Unidos. Se llegó a implantar también en Inglaterra y en Japón, con los nombres TACS y MCS-L1 respectivamente. WIKIPEDIA. Sistema Telefónico Móvil Avanzado. [en línea] <http://es.wikipedia.org/wiki/Sistema_Telef%C3%B3nico_M%C3%B3vil_Avanzado> [consulta: 22 enero 2015]

⁶⁶ BARRÍA, SUSANA. “Webmóvil: desarrollo de soporte comunicacional web a través de dispositivos de telefonía móvil”. op. cit., p. 13

áreas económicas de influencia, la que posteriormente se expandió por casi todo el globo, masificando exponencialmente el uso de teléfonos celulares de 2G.

Los sistemas de comunicaciones móviles 2G utilizan protocolos de codificación más sofisticados y se emplea en los sistemas de telefonía celular actuales. El sistema GSM (Global System for Mobile Communication)⁶⁷, es la base de la tecnología que hace posible este avance en la industria de la telefonía móvil, ya que, utiliza modulación digital para mejorar la calidad de la voz, además de la calidad de la transmisión y la cobertura. Los protocolos empleados en los sistemas 2G soportan velocidades de información, como señalamos, más altas por voz, pero limitados en comunicación de datos (“*banda estrecha*”). Sin embargo, uno de los hitos más grandes de la telefonía móvil se llevó a cabo en 2G, y estos es el desarrollo de los mensajes de texto o SMS (Short Message Service). Además, esta tecnología permite ofrecer servicios adicionales a los usuarios como fax y buzón de voz⁶⁸. Existió un periodo de transición entre la tecnología de segunda generación y tercera generación, introducida a finales de los años 90, y que se denominó 2.5G.

La generación 2.5G ofrece características extendidas, ya que cuenta con más capacidades adicionales que los sistemas 2G. Esta fase utilizaba el estándar GPRS⁶⁹, el cual permitía a los usuarios enviar datos con imágenes y/o gráficos. La importancia de este servicio creció conjuntamente con el desarrollo del internet y los protocolos

⁶⁷ Esta tecnología es explicada en el punto 2.2.4.1.1 de este capítulo.

⁶⁸ DE BERNARDO, CESAR. y PRIEDE, TIZIANA. op. cit., p. 3

⁶⁹ Esta tecnología es explicada con detalle en el punto 2.2.4.1.2 de este capítulo.

de internet (IP)⁷⁰. La red EDGE (Enhanced Data Rates for Global Evolution)⁷¹, la cual es explicada con mayor detalle más adelante, es la evolución del GPRS. Puede ser usado en cualquier transferencia de datos basada en conmutación de paquetes (*Packet Switched*) como lo es la conexión a internet. La red EDGE permite a los usuarios visualizar en sus teléfonos móviles, aplicaciones que requieran una velocidad de transferencia de datos, o ancho de banda altos, como videos u otros servicios multimedia. EDGE es un ejemplo de tecnología 2.5G, sin esta red los smartphone o teléfonos inteligentes no existirían⁷².

2.2.4.1 Transferencia de datos en 2G⁷³

Como vimos, la segunda generación de teléfonos móviles podemos dividirla en 2G propiamente tal, y 2.5G como una etapa intermedia anterior al desarrollo de la red de 3G. La diferencia entre 2G y 2.5G no es menor, ya que, en cuanto a sistema de transferencia de datos, 2.5G significa un avance sustantivo en comparación a su antecesor⁷⁴.

⁷⁰ IP, es un protocolo de comunicación de datos digitales, permite la transmisión de datos a través de paquetes conmutados o datagramas desde distintas direcciones. Básicamente el IP lo que hace es enviar cada archivo como varias partes, pequeños datos, sin garantizar su destino final pero tratando de buscar la mejor ruta conocida entre los dispositivos conectados. Luego estos paquetes serán ensamblados al llegar a su destino, convirtiéndose en el archivo final que queríamos obtener.

⁷¹ Esta tecnología es explicada con detalle en el punto 2.2.4.1.3 de este capítulo.

⁷² LÓPEZ, NICOLÁS. 2011. Efecto de las redes de cuarta generación (LTE) en los servicios móviles en Chile. [en línea] < http://www.tesis.uchile.cl/bitstream/handle/2250/104136/cf-lopez_nm.pdf?sequence=3 > [consulta: 22 enero 2015]

⁷³ LÓPEZ, NICOLÁS. “Efecto de las redes de cuarta generación (LTE) en los servicios móviles en Chile”. op. cit., p. 6-11

⁷⁴ BASOALTO, REBOLLEDO. 2007. Administración de mensajería de texto en cascada para teléfonos celulares [en línea] <http://www.tesis.uchile.cl/tesis/uchile/2007/basoalto_cr/html/index-frames.html> [consulta: 22 enero 2015]

2.2.4.1.1 GSM

Global System for Mobile Communicatios (Sistema Global para las Comunicaciones Móviles). Es el sistema de teléfono móvil digital más utilizado en el mundo. La mayoría de las redes GSM utilizan 900MHz y 1800MHz en los Estados Unidos, pero en casi todo el mundo se prefiere 850MHz y 1900MHz⁷⁵. Los teléfonos GSM funcionan con una triple banda y pueden ser utilizados en Europa, EE.UU., y muchos otros países en el mundo. Con el sistema GSM se permite alcanzar velocidades de transmisión de hasta 9600bps (bits por segundo), lo que permite la transmisión de datos ligeros como los conocidos SMS.

2.2.4.1.2 GPRS

Como evolución de GSM surgen tecnologías como GPRS o EDGE, que configuran la llamada 2.5G.

GPRS son las siglas para: *General Packet Radio Service* (Servicio General de Paquetes vía Radio). Es una extensión del GSM para la transmisión de datos conmutados o por paquetes (como lo es la conexión a internet). Este sistema permite

⁷⁵ En Chile GSM: Movistar/Claro (850Mhz/1900Mhz), Entelpcs (1900Mhz).

velocidades de transferencia de 56 a 144Kbps (kilobits por segundo), aunque en la práctica solo alcanza los 80Kbps, es decir, 0,08 “Megas” de velocidad. GPRS es un sistema probado y por lo tanto muy confiable para el uso estándar de datos móviles, ajustándose a las necesidades básicas de transferencia de datos de un usuario de telefonía móvil. Para entenderlo mejor, este sistema de tecnología móvil, es el que permite los primeros accesos a internet en los equipos móviles.

2.2.4.1.3 EDGE

Acrónimo para *Enhanced Data Rates for GSM of Evolution* (Tasas de Datos Mejoradas para la evolución de GSM), también conocida como EGPRS. Esta tecnología de telefonía móvil celular, es la evolución de la GPRS. Permite un máximo de conexión de 236Kbps, es decir 0,236 “Megas” (con lo que triplica la velocidad alcanzada en una tecnología GSM). Si un Smartphone es compatible como EDGE, puede ser utilizado para la transmisión de datos móviles “pesados”, como la recepción de grande archivos adjuntos de correo electrónico, navegar por páginas web complejas a gran velocidad, ver videos y acceder a otros servicios multimedia. Esta tecnología es muy utilizada por los proveedores de telefonía celular, ya que, entrega casi las mismas ventajas que una tecnología 3G más sofisticada ocupada por teléfonos celulares inteligentes (como UMTS), a un menor precio de implementación y mantención, lo que hace que una gran cantidad de operadores de telefonía móvil celular tengan implementada la tecnología EDGE, dominando el mercado global de las comunicaciones GSM/GPRS.

2.2.5 Tercera generación de teléfonos móviles (3G)⁷⁶

Uno de los mayores hitos en la historia de la telefonía móvil se vivió el año 2001, ya que, en ese año, se supone la aparición de los primeros celulares que incorporaban una pantalla LCD a color, hecho que abría un inmenso abanico de posibilidades en cuando a nuevas funciones y aplicaciones en el ámbito móvil.

Todo este conjunto de nuevos servicios integrados en el terminal, fue posible gracias a la implementación de una tecnología digital de datos conmutados capaz de crear las vías de transferencia necesarias para la utilización de estos avances. Que importa, por ejemplo, desarrollar el auto más rápido del mundo, si no hay ninguna carretera donde este pueda “correr”, que soporte esta velocidad y donde este auto se pueda utilizar. Lo mismo ocurre en esta situación, ya que tanto desarrollo de aplicaciones y servicios no es posible sin la existencia de una red capaz de entregar el suficiente ancho de banda, suficientemente rápido, para hacer posible su utilización y disfrutar de estos beneficios. He aquí que junto con este desarrollo vino también el de un nuevo estándar para la transferencia de datos, uno capaz de llevar a cabo esta infinidad de posibilidades, la *Universal Mobile Telecommunication System* (UMTS⁷⁷).

⁷⁶ LÓPEZ, NICOLÁS. “Efecto de las redes de cuarta generación (LTE) en los servicios móviles en Chile”. op. cit., p. 12-19

⁷⁷ UNION EUROPEA. Introducción Coordinada De Un Sistema De Comunicaciones Móviles e Inalámbricas De Tercera Generación (UMTS) En La Comunidad. [en línea] <http://europa.eu/legislation_summaries/other/l24202_es.htm> [consulta: 22 septiembre 2014]

2.2.5.1 Transferencia de datos en 3G

2.2.5.1.1 UMTS

UMTS⁷⁸, es la principal tecnología usada por los móviles de tercera generación o 3G. Los servicios asociados con la 3G proporcionan la posibilidad de transferir datos con una velocidad de acceso a Internet elevada, lo que permite transmitir sin problemas audio y video en tiempo real entre una variedad de otros servicios como; la descarga de programas, intercambio de email, mensajería instantánea, utilización de diversas aplicaciones, etcétera. Permite velocidades de conexión de 0.2Mbps (Megabits por segundo) y 0.4Mbps, lo que nos permite en cuestión de segundos enviar y recibir contenidos de gran cantidad de bits. El UMTS puede funcionar en varias frecuencias, entre los 450 y los 2600 MHz⁷⁹.

Como señalamos, tras la implementación del sistema UMTS, el concepto de telefonía móvil ha cambiado radicalmente, pasando de ser un elemento que permitía la más simple comunicación en movimiento, para convertirse en un terminal multimedia con un sin fin de capacidades tanto para la comunicación como para el ocio. Lo anterior significa que pequeños aparatos simplificaran significativamente

⁷⁸ Es el acrónimo para *Universal Mobile Telecommunication System* (Servicios Universales de Comunicaciones Móviles).

⁷⁹ En Chile UMTS 3G: Movistar/Claro (850Mhz), Entelpcs (1900Mhz). Nextel, VTR Móvil (1700/2100Mhz).

nuestras vidas, con una cantidad ilimitada de servicios y aplicaciones, capaz de satisfacer hasta las más pequeñas necesidades, permitiéndonos estar altamente comunicados, y compartir con otros, incluso, cada segundo de nuestras vidas.

2.2.5.1.2 EV-DO

De las siglas inglesas *Evolución-Data Optimized o Evolution-Data Only*, es una versión avanzada de la tecnología móvil CDMA2000, la segunda más usada del mundo.

La velocidad que permite conseguir esta tecnología está entre los 0.4 y 0.7Mbps en las versiones iniciales. Otras más modernas alcanzan valores muy superiores a los especificados. Esta versión podría fácilmente considerarse como una 3.5G por su velocidad de transmisión de datos.

2.2.6 Cuarta generación de teléfonos móviles (4G)⁸⁰

La cuarta generación utiliza sistemas LTE-Avanzado, LTE, HSPA+ y WiMAX o WiMax Avanzado. LTE-Avanzado es la mejor tecnología existente hoy

⁸⁰ LÓPEZ, NICOLÁS. “Efecto de las redes de cuarta generación (LTE) en los servicios móviles en Chile”. op. cit., p. 19-32

en día en el mundo en cuanto a transferencia de datos. Todos los datos, incluyendo la voz de una llamada, son transmitidas por intermedio de paquetes conmutados con una velocidad que estará entre los 100Mbps y 1Gbps⁸¹ (Gigabits por segundo)⁸².

Este sistema de cuarta generación es capaz de operar en múltiples bandas de frecuencia, incluyendo las ocupadas por 2G y 3G, lo que le permite utilizar de mejor manera el espectro disponible, asegurando la estabilidad de conexión y una mayor área de cobertura⁸³. Su LTE avanzado, permite un mejor desempeño al establecer una conexión en movimiento⁸⁴. Además incorpora un método de acceso que logra aumentar la velocidad de transferencia dependiendo del número de antenas que se agreguen. Este sistema comenzó a ser comercializado a partir del año 2013 en el mundo. Con el LTE-Avanzado es posible alcanzar velocidades de descarga de entre 10 y 300Mbps en función de su categoría. Fue implantado primeramente en países como Estados Unidos, Brasil y Alemania.

En definitiva, en comparación a la arquitectura de su predecesor, el sistema LTE-Avanzado de cuarta generación, permite una: a) reducción de latencia o retardos temporales dentro de la red, debido a un único nodo en la interfaz aérea; b) mejor calidad en la conexión de la comunicación; c) mayor estabilidad en la conexión de la comunicación; d) mayor cobertura; e) mayores índices de transferencia de datos, lo

⁸¹ 1000Mbps

⁸² Con estos valores por ejemplo, a través de un teléfono móvil o celular, es posible obtener una perfecta recepción para la televisión *high definition* o de alta resolución.

⁸³ Una celda LTE ofrece un rendimiento óptimo para un radio de hasta 5 km, un rendimiento efectivo para un radio de hasta 30 km y rendimiento limitado en torno a 100 km. Gracias a este aumento de las capacidades de cobertura, se necesitarían una menor cantidad de estaciones bases para cubrir un área.

⁸⁴ A pesar de que el sistema está creado para operar de manera óptima a velocidades de 15 km/h, puede hacerlo hasta una movilidad de 350 km/h sin perder la conexión.

que le permitiría ofrecer servicios de cualquier clase en cualquier momento, en cualquier lugar.

2.3 Sistema operativo móvil

2.3.1 ¿Qué es un sistema operativo?

Cuando damos una mirada hacia atrás y vemos la historia de la humanidad, lo primero que podemos apreciar es la notoria evolución de la sociedad. Nuestro planeta ha sido testigo de cómo el hombre con sus manos y pies sobre la tierra, se ha erguido al punto de alcanzar las estrellas.

Los primeros hombres, según la teoría de la evolución, eran más parecidos a un primate, que con el tiempo fueron evolucionando hasta alcanzar lo que hoy conocemos como el hombre moderno o el “hombre pensador” (*homo sapiens*). Sin embargo, el adjetivo “sapiens” no es más que un intento por diferenciar un tipo de hombre mucho más “estilizado” a nuestros ojos que los anteriores, un ser menos animal y más parecido a un hombre actual. Sin dudas, que atribuirle a esta especie de hombre la calidad exclusiva de pensante, no sería más que un dejo de vanidad de nuestra parte, de hecho, una de las principales cualidades del pensamiento es la de poder desarrollar tecnología, y desde ya decimos, la tecnología estuvo presente en todas las etapas de la evolución humana.

La RAE define tecnología como un: *1. f. Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico. 2. f. Tratado de los términos técnicos. 3. f. Lenguaje propio de una ciencia o de un arte. 4. f. Conjunto de los instrumentos y procedimientos industriales de un determinado sector o producto.* La tecnología es la aplicación práctica de un conocimiento, la Real Academia Española dice “conocimiento científico”, pues, entiende a la ciencia⁸⁵ como algo especializado, un “conocimiento especializado”. Sin embargo, un conocimiento de por sí es una inteligencia⁸⁶, y en este sentido la sola aplicación de la inteligencia es tecnología.

Un Sistema Operativo (SO) es una tecnología, porque es una herramienta desarrollada a través de la aplicación de un conocimiento. Específicamente un SO es “*un conjunto de programas encargados de administrar y explotar los recursos de un sistema de computador para ofrecer un conjunto de servicios a los usuarios (...) Podemos ver el sistema operativo como un encargado de asignar los recursos*”⁸⁷, “*el soporte lógico imprescindible para convertir el soporte físico de un computador en una máquina utilizable por el usuario*”⁸⁸.

⁸⁵ Real Academia Española, “*Definición de Ciencia: 1. f. Conjunto de conocimientos obtenidos mediante la observación y el razonamiento, sistemáticamente estructurados y de los que se deducen principios y leyes generales. 2. f. Saber o erudición. Tener mucha, o poca, ciencia. Ser un pozo de ciencia. Hombre de ciencia y virtud. 3. f. Habilidad, maestría, conjunto de conocimientos en cualquier cosa. La ciencia del caco, del palaciego, del hombre vividor. 4. f. pl. Conjunto de conocimientos relativos a las ciencias exactas, fisicoquímicas y naturales. Facultad de Ciencias, a diferencia de Facultad de Letras*”.

⁸⁶ Real Academia Española, “*Definición de Conocimiento: 2. m. Entendimiento, inteligencia, razón natural*”.

⁸⁷ ORTIZ PABÓN, HÉCTOR. 2005. Sistemas Operativos Modernos. [en línea] <http://books.google.es/books?id=3Hb6f3gyCxUC&pg=PA11&hl=es&source=gbs_toc_r&cad=3#v=onepage&q&f=false> [consulta: 22 enero 2015]

⁸⁸ MARTINES, P., CABELLO, M. y DÍAZ MARTÍN, J. 1997. Sistemas Operativos: teoría y práctica. [en línea] <<https://books.google.es/books?id=wXzwFPaVku0C&printsec=frontcover&dq=SISTEMAS+OPERATIVOS+Y+TEORIA+PRACTICA&hl=es&sa=X&ei=ChTLVKXsIrWJsQTfgYLYCQ&ved=0CCIQ6AEwAA#v=onepage&q=SISTEMAS%20OPERATIVOS%20Y%20TEORIA%20PRACTICA&f=false>> [consulta: 22 enero 2015] p.1

El objetivo primordial del sistema operativo es proporcionar comodidad al usuario, permitir que la utilización del computador se pueda hacer de una manera más rápida y simple. También como un segundo objetivo, el SO busca otorgar eficiencia en el uso del computador⁸⁹. Y un tercer objetivo, es el de permitir que el computador sea una maquina segura y fiable⁹⁰.

En resumen el SO es un programa (*software*⁹¹) complejo que facilita el uso del soporte físico (*hardware*⁹²) de un computador⁹³. Lo anterior implica que un computador necesita un sistema operativo para funcionar, pero no todo sistema operativo sirve para cualquier computador, ya que, un sistema operativo tiene indicaciones para trabajar con los recursos de un computador, y si un computador no tiene los recursos que necesita el SO para hacer algo, las funciones de este sistema operativo no se podrán llevar a cabo, haciendo que algunas tareas no funcionen o funcionen de manera deficiente a lo normal. Es por esto que existen una gran cantidad de sistemas operativos, así como también existen una gran variedad de computadores.

⁸⁹ La eficiencia está directamente relacionada con la gestión de recursos del sistema, resolviendo los conflictos de asignación y liberación de recursos al ejecutar alguna aplicación.

⁹⁰ La fiabilidad está relacionada con la separación y la máquina, de manera que ciertos errores sean subsanados por el sistema, sin informar al usuario.

⁹¹ El *Software* son los programas, lo intangible del computador, ya que se encuentran de forma codificada como ceros y unos (código binario) no visibles por los usuarios, y almacenados dentro de la memoria principal del computador, o en el disco duro, o en memorias externas (CD-ROM, DVD, pendrive, tarjeta SD, tarjeta mini SD, etcétera).

⁹² El *Hardware* es lo tangible del computador. En un teléfono móvil básicamente está formado por la unidad central en donde se encuentra la memoria, la pantalla, el teclado, el video cámara.

⁹³ Este trabajo no pretende explicar de manera más profunda ni de la informática lo que es un sistema operativo, basta saber para estos efectos que es un programa que permite que pueda funcionar un computador, en este caso, el teléfono móvil.

2.3.2 Sistemas operativos más utilizados en el mundo

Un Sistema Operativo como vimos, es un programa complejo, que requiere altos conocimientos informáticos en cuanto a programación, que es el lenguaje en el cual se crean o escriben los programas o *software* en general.

Lo anterior implica que no todo el mundo tiene la capacidad y conocimientos técnicos para crear un sistema operativo que es básico para el funcionamiento de un computador. En este sentido, existen algunas personas en el mundo que se han encargado de desarrollar distintos sistemas operativos para los computadores en el mundo. Pero como señalamos, existe una gran variedad de computadores, algunos con mayores o menores capacidades físicas que otros, y así también con finalidades distintas (hoy en día por ejemplo, un Smartphone es un teléfono celular y una computadora a la vez, dos cosas distintas pero que deben funcionar al mismo tiempo sin interferir una con otra, de esta manera necesitara un sistema operativo que le permita llevar a cabo estas dos tareas de manera simple y eficiente), lo que hará que también existan distintos sistemas operativos con finalidades diametralmente distintas.

Alguno de los Sistemas Operativos más famosos y utilizados en el mundo por su simplicidad, seguridad y eficiencia son:

- **DOS:** Es uno de los primeros sistemas operativos para PC. Su nombre está compuesto por las siglas *disk operating system* (sistema operativo de disco). Fue creado originalmente para las computadoras IBM, las IBM PC, que utilizaban procesadores de 16 bits⁹⁴. Este sistema operativo contaba con una interfaz de línea de comando y fue el antecesor del sistema operativo MS-DOS de Microsoft.
- **UNIX:** Es un sistema operativo portable, multitarea y multiusuario. Es desarrollado en 1969 por Laboratorios Bell de AT&T. Lo especial de este sistema operativo, es su capacidad de poder utilizarse tanto en PC como en computadores portátiles (Laptops), y fue la base para otros sistemas operativos para equipos móviles.
- **Microsoft Windows:** Es el nombre de una familia de sistemas operativos creados por las empresas Microsoft el 20 de noviembre de 1985 como un complemento para el sistema operativo MS-DOS para darle una interfaz gráfica de usuario en vez de la tradicional línea de comando. Windows es el sistema operativo más utilizado en el mundo. Cuenta con más de una docena de versiones y se actualiza a medida que el hardware de los PC también evoluciona. El 26 de octubre del 2012 Microsoft lanzo Windows 8, el primer sistema operativo capaz de utilizarse tanto en PCs como en Tablet. Windows poseía un sistema operativo creado para teléfonos móviles, el llamado “Windows Mobile”, pero su baja aceptación y la creciente competencia hizo que Windows perdiera una gran participación de mercado. Buscando una

⁹⁴ Hoy en día los computadores alcanzan los 32 o 64 bits según sistema operativo.

nueva imagen en este mercado la empresa creó “Windows Phone” un sistema operativo mucho más acorde a las exigencias del usuario y con una interfaz familiar (similar a las utilizadas por otros SO más populares en telefonía móvil). Junto con el lanzamiento de Windows 8, Microsoft también lanzó Windows Phone 8, un SO enfocado en Smartphone de la más alta tecnología.

- **LINUX:** Linux es un núcleo libre de sistema operativo basado en Unix. Lo que hace tan popular a Linux entre los usuarios de todo el mundo, es que es el principal ejemplo de Software Libre. Linux es un sistema operativo que se ha ido desarrollando por los mismos usuarios que han ido programando libremente Linux, desarrollando software utilizable exclusivamente para este SO. En general este SO es completamente programable, puede ser modificado sin que exista ningún límite para ello. Debido a que la programación de un SO es compleja, Linux es un SO muy popular entre informáticos, programadores y personas con un alto nivel de conocimiento en estas áreas.
- **MacOS:** del inglés Macintosh Operating System (Sistema Operativo de Macintosh) es el nombre del sistema operativo creado por la empresa Apple para su línea de computadoras Macintosh. MacOS fue desarrollado en 1985 y su principal objetivo fue la de crear un SO basado en MS-DOS mucho más simple de utilizar para el usuario. En 1999 pasó a utilizar Unix para seguir desarrollando y muchos de sus elementos originales pasaron a transformarse debido a este cambio. Actualmente MacOS es el segundo sistema operativo más utilizado en el mundo (detrás de Microsoft). Sus versiones de MacOS han

ido actualizándose con el desarrollo de la tecnología Hardware de los computadores.

- **iOS:** Este SO nació con el nombre de iPhone OS, para luego denominarse solo IOS. Es un sistema operativo de la empresa Apple desarrollado originalmente para el iPhone, el primer teléfono inteligente multimedia con conexión a internet, pantalla táctil capacitiva y escasos botones físicos desarrollados por Apple. Este sistema operativo luego fue utilizado por toda la gama de dispositivos portables de Apple, como el iPod Touch, iPad y el Apple TV. Fue lanzado el 9 de enero de 2007.
- **BlackBerry OS:** Sistema Operativo creado y utilizado para la línea de teléfonos inteligentes BlackBerry, desarrollado por la compañía canadiense Reseach In Motion (RIM). El primer BlackBerry smartphone fue lanzado al mercado el año 2002 y soportaba correo electrónico, telefonía móvil, mensajería de texto, faxes por Internet, navegación web y otros servicios informáticos inalámbricos. Lo que caracteriza a este tipo de celulares es su teclado QWERTY incorporado (teclado común de computadora).
- **Symbian OS:** Es un sistema operativo producto de la alianza de varias empresas de telefonía móvil, entre ellas Nokia, Sony, Samsung, Siemens, Motorola, LG, Lenovo, Benq, entre otras. Symbian Ltd. se fundó el 24 de junio de 1998 y su principal objetivo fue crear un SO para teléfonos móviles que pudiera competir en ese tiempo con el de Palm o Windows Mobile de Microsoft. Actualmente es Nokia quien comercializa la mayoría de los

móviles con Symbian⁹⁵, sin embargo, el año 2011 Nokia traspasa los derechos de soporte y desarrollo de sistemas a la empresa multinacional Accenture Limited. Nokia señaló que solo desarrollaría Symbian hasta el año 2016 debido a la alta competencia que les ha presentado iOS y Android⁹⁶.

- **ANDROID**⁹⁷: Androide en español, es un sistema operativo basado en Linux enfocado para ser utilizado en dispositivos móviles como teléfonos inteligentes, tabletas y otros dispositivos. Android fue desarrollado y luego revelado el 5 de noviembre de 2007 por la Open Handset Alliance (OHA), una alianza comercial de 84 compañías entre las que se encuentran Google (con la mayor participación), Motorola, Samsung, LG, Dell, Intel, etcétera. Este Sistema Operativo cambio el paradigma, ya que al ser un SO libre, permitió que los usuarios desarrollaran software o aplicaciones (las llamadas “.app”) para los teléfonos con Android.

2.4 Internet móvil

2.4.1 Internet

⁹⁵SMARTGSM MOBILE WORLD. Que Es Symbian: Todos Los Celulares. [en línea] <<http://www.smartgsm.com/guias/articles/view/que-es-symbian-todos-los-celulares>> [consulta: 09 septiembre 2014]

⁹⁶XATAKA MÓVIL. 2012. Nokia y el cada vez más oscuro futuro de Symbia. [en línea] <<http://www.xatakamovil.com/nokia/nokia-y-el-cada-vez-mas-oscur-o-futuro-de-symbian>> [consulta: 22 enero 2015]

⁹⁷ ANDROID. 2012. Discover Android. [en línea] <<http://www.android.com/about/>> [consulta: 22 enero 2015]

Para poder entender que es Internet Móvil es necesario tener una pequeña idea de lo que es y cómo funciona Internet.

A grosso modo Internet es un conjunto descentralizados de redes de comunicación (un conjunto de equipos informáticos y software conectados entre sí, a través de los cuales básicamente se puede compartir información, recursos y ofrecer servicios) interconectados, que utilizan un conjunto de reglas TCP/IP de transmisión de datos, garantizando que las redes físicas heterogéneas que la componen, funcionen como una sola red lógica de alcance mundial. Uno de los servicios más utilizados en Internet ha sido la Word Wide Web (www o “la Web”), que es un conjunto de protocolos que permite de forma sencilla, consultar de manera remota archivos de hipertexto (páginas web). Existen también otros servicios y protocolos en Internet a parte de la Word Wide Web, como lo son el envío de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la transmisión de contenido de comunicación multimedia de telefonía (VoIP), televisión (IPTV), acceso remoto a otros dispositivos (SSH y Telnet) o juegos en línea entre otros.

2.4.2 ¿Qué es internet móvil?⁹⁸

⁹⁸WIKIPEDIA. Telefonía móvil. [en línea] <http://es.wikipedia.org/wiki/Telefon%C3%ADa_m%C3%B3vil#Conexi.C3.B3n_a_Internet> [consulta: 22 enero 2015]

Desde la implementación de la Segunda Generación, los usuarios experimentaron la posibilidad de conectarse a Internet a través de sus celulares. Las nuevas tecnologías, permitieron que ellos pudieran realizar a través de sus aparatos móviles pequeñas tareas a través de internet como; mandar o recibir datos de baja capacidad en bits, navegar por algunas páginas web o escribir mails. Esta posibilidad de conectarse a Internet a través de los teléfonos celulares fue conocida como la “Internet Móvil”.

La Internet Móvil es un servicio que permite a los usuarios de teléfonos celulares que soporten tecnología 2G, 3G y 4G, usar Internet a través de sus Smartphone o no Smartphone. Los usuarios consumidores de internet hasta la implementación de la Internet Móvil, solo podían conectarse a ella, a través de una conexión residencial directamente a un computador o CPU. La Internet Móvil también permitió la conexión inalámbrica de internet hacia equipos portátiles o Laptops, lo que masifico aún de mayor manera su utilización y demanda.

Hoy en día, dependiendo de la tecnología del equipo móvil y la sistemas tecnológicos implementados en cada país, es posible obtener una velocidad de navegación de banda ancha en nuestros celulares, que nos permite realizar las más variadas tareas en ellos, pudiendo rápidamente acceder a todo contenido en la Internet como si estuviéramos haciéndolo a través de un computador, con la ventaja de la movilidad que nos brinda hacerlo a través de un teléfono móvil.

2.4.3 El dilema de la transferencia de datos

Una de las mayores ventajas que nos supone la utilización de la Internet en nuestros Smartphone o no Smartphone, es la capacidad de transmitir información de manera rápida y de cualquier lugar a través de ellos. Esto supone en el mundo vertiginoso de hoy, una mayor productividad en las personas, ya que la posibilidad de realizar tareas en casi cualquier lugar, permite en teoría un mejor aprovechamiento del tiempo y rendimientos mucho mayores, no teniendo que esperar llegar a un computador con acceso a internet para conectarnos a él. Además, con la creación de los Smartphone o teléfonos inteligentes, el abanico de oportunidades aumenta, haciendo que hoy en día todo computador sea totalmente prescindible, ya que, en sí mismos nuestros teléfonos celulares representan verdaderos “computadores portátiles”.

Sin embargo, esta virtud del Internet Móvil, en una era de computadores portátiles, hace que nuestros móviles estén expuestos casi a las mismas situaciones a la que estaban expuestos nuestros computadores con acceso a internet. Virus informáticos, robo de datos personales, suplantación de identidad, son solo alguno de los problemas a los que nos encontrábamos expuestos al navegar por internet, pues, nuestros computadores mantenían una gran cantidad de información sobre nosotros y nuestros hogares, que podía ser fácilmente vulnerados con aquellos con los conocimientos para hacerlo, e incluso sin los conocimientos pero con software

fácilmente utilizables por un usuario promedio. Ahora, sabiendo todos los datos que nuestros celulares tienen y recogen de nosotros; fotos, videos, contactos, claves, conversaciones, llamadas, localización, etcétera, imagina cuanta información nuestros móviles tienen, y cuan fácil podría hoy en día ser, que otros tuvieran acceso a ellos. El problema radica no solo en la posibilidad de que esto pueda suceder, sino en la situación de que de ser así, sea esto perfectamente legal. Todo esto lo veremos con mayor detalle en el capítulo a continuación.

CAPITULO III

PRIVACIDAD Y TELEFONÍA MOVIL

3.1 El riesgo de Hansel y Gretel

Desde la invención del teléfono en 1876 y la invención del radio en la década de 1880⁹⁹, han transcurrido aproximadamente ciento treinta años. En todo este tiempo, el mundo ha alcanzado un desarrollo tecnológico inimaginado y consecuentemente con ello, un sin fin de desafíos. La telefonía celular ha sido uno de estos logros impensados, ya que en muy poco tiempo, el mundo logro asombrarse con la invención del teléfono celular, para que en el siglo XXI, maravillare con los llamados smartphone o teléfonos inteligentes.

Sin dudas, la carrera de la telefonía móvil ha sido una de las más prosperas para la humanidad, permitiendo que unos simples aparatos que permitían la comunicación sin un terminal fijo, se convirtieran en verdaderas computadores móviles, capaz de realizar hasta las tareas más difíciles, sin requerir nada más que un pequeño aparato de bolsillo. La comodidad que supone poder llevar un verdadero PC de bolsillo son a toda vista infinitas, ya que, permite que las personas puedan en todo

⁹⁹ El teléfono y el radio son los principales inventos que permiten luego la creación de la telefonía celular en los años 50.

lugar y en todo momento, comunicarse, subir o descargar contenido multimedia, realizar tareas o trabajos, fotografiar o grabar casi cualquier momento, jugar, acceder a su email, interactuar con casi cualquier persona en el mundo, etcétera. Y todo esto sin mayores costos de los que supone adquirir un teléfono y en algunos casos una conexión a internet.

En el famoso cuento alemán de los hermanos Grimm, Hansel y Gretel, se trata de dos pequeños hermanos abandonados a su suerte en el bosque por sus pobres padres. Después de dos días perdidos, Hansel y Gretel se encuentran con una casita en medio del bosque hecho completamente de dulce. Maravillados, los hermanos comenzaron a comer la casita de dulce sin percatarse, que esta era una trampa de una vieja bruja para encerrarlos, y luego comerlos. La enseñanza de este cuento sería a dudar de todo lo que pueda parecer demasiado bueno, porque podría traer consigo un mal que pueda ser mucho mayor.

La referencia a esta historia no es un desvarío mental del autor de este trabajo, sino un ejercicio didáctico para darnos cuenta que no todo lo que parece demasiado bueno, tiene que necesariamente serlo, o como dice el refrán; “no todo lo que brilla es oro”. Sin duda, que el mundo maravillado por el avance de la telefonía móvil, no se ha percatado de todo lo que este desarrollo puede significar negativamente para nuestras vidas, sin duda, dirán algunos, todo desarrollo tiene también sus costos. Muy bien lo saben hoy Hansel y Gretel que para poder comer sin haberlo hecho durante dos días, corrieron a comer la casita de dulce, sin cuestionar tan asombroso hecho, y no lo cuestionaron por una sencilla razón, el riesgo valía la oportunidad de salvar sus vidas. Algo parecido también sucede en el caso de la Telefonía Móvil, ya que, para

muchos el beneficio de tener un Móvil es tan superior, que justificaría cualquier riesgo, sin embargo, ¿vislumbra el usuario verdaderamente ese riesgo?, y si ese riesgo fuera mucho mayor que el beneficio, ¿pensaría igual?

3.2 El riesgo a la privacidad

Así como en su momento la invención del Computador Personal o PC trajo sendos dilemas en cuanto a la protección de la información contenida en ellos, y más aún, esta discusión aumento con la creación de la Internet. También de este modo la telefonía móvil como hoy la conocemos, ha generado grandes debates en cuanto a la intromisión que generan estos aparatos en la privacidad de las personas. Basta pensar unos segundos en toda la información que contienen nuestros móviles, todo lo que se puede saber de nosotros, como estos captan cada segundo de nuestras vidas, y cuan fácil sería que al perder nuestro teléfono móvil, otro se hiciera con toda esta información, nuestra vida.

El problema con la extensión y progresiva sofisticación de los teléfonos móviles inteligentes, es que cuanto mayor es la capacidad de ellos de realizar nuestras tareas, más vulnerables nos volvemos, pues, mayores son los alicientes para que terceros se hagan con el contenido dentro de ellos y utilizarlos en su beneficio. El perjuicio sería para nosotros, perder nuestra privacidad, nuestra intimidad, nuestros secretos.

El desarrollo de la tecnología en la telefonía móvil vislumbra un futuro con nuevos y mejores aparatos móviles. Aún es insospechado los límites de este vertiginoso avance y no hay nada que suponga que esto no continuara así. El hombre naturalmente crece y se desarrolla, y así también lo hace el mundo a su alrededor. Las personas tienen necesidades y buscan satisfacerlas, el hombre quería poder comunicarse y creo el teléfono, quería escuchar a otros desde otras latitudes y creo la radio, y cuando estas dos necesidades se volvieron una y junto a ella se buscó mayor libertad, creo la telefonía celular. Pero debemos recordar, que en la teoría del Leviatán de Hobbes, el hombre entrego parte de su libertad en busca de satisfacer otra necesidad, la seguridad, y es esta seguridad la que busca el derecho al regular nuestra actividad. De esta forma, es preciso fijar un marco normativo donde las personas puedan acceder a todas las virtudes de esta tecnología, pero a la vez, estar seguras que esto no interferirá la esfera de su privacidad. Ciertamente todo avance tiene sus costos, y la tecnología no escapa a esta paradoja, un ejemplo extremo es la investigación de la fusión de átomos por Albert Einstein, que permitiría producir energía ilimitada, pero que termino transformándose en una de las armas de destrucción masiva más letales para el mundo¹⁰⁰.

Pero si lo pensamos un poco, cuanto poder tendría aquel o aquellos si tuviera todo tipo de información, nuestros datos personales; que hacemos, que queremos, que nos gusta, con quien nos juntamos, nuestros secretos más sensibles, en las manos de una sola persona, o en las manos de un grupo de ellas, saber quiénes somos mejor que nosotros mismos, ¿no es acaso ese un poder muy grande? ¿ el poder de Dios? ¿la

¹⁰⁰CLARÍN. 2012. Einstein, lleno de culpa por la bomba atómica. [en línea] <<http://edant.clarin.com/diario/2005/07/04/sociedad/s-03601.htm>> [consulta: 09 septiembre 2014]

omnipresencia? No es tan absurda esta idea considerando que empresas gastan millones de dólares en obtener algunos datos sobre nosotros. Es por esto que se hace tan necesaria una legislación al respecto, que resguarde de manera efectiva nuestros derechos, nuestra libertad, nuestra seguridad.

CAPITULO IV

PROTECCIÓN DE DATOS EN CHILE

4.1 Historia de la protección de datos personales en Chile¹⁰¹

En nuestro país diversos cuerpos normativos se refieren directa o indirectamente a la protección de los datos de carácter personal. La protección a la vida privada frente a las nuevas tecnologías no fue tratada por los redactores de la Constitución Política de 1980, pues, no existía en la comunidad jurídica y académica chilena una mayor preocupación por la protección de datos personales. No fue sino hasta a mediados de los años 80 que se comienza a esbozar los primeros intentos por regular el fenómeno y las implicancias de la informática en nuestro país, básicamente por dos factores: en primer lugar, por el proceso de modernización económica, y en segundo término, muy ligado al anterior, por el inicio de actividades, desde fines de la década de los 70 de empresas dedicadas a informar sobre la solvencia económica de las personas. Dichas circunstancias fueron determinantes en la regulación de los efectos de la informática en Chile, el hecho de establecer algunos límites al funcionamiento de las empresas dedicadas a informar sobre la solvencia económica de las personas.

¹⁰¹ ANGUITA RAMÍREZ, PEDRO. 2007. La protección de datos personales y el derecho a la vida privada: Régimen jurídico, jurisprudencia y derecho comparado. Santiago de Chile, Editorial Jurídica de Chile. 627p.

4.1.1 Anteproyectos de ley elaborados durante el régimen militar

Durante el régimen militar (1973-1990) se elaboraron tres proyectos de ley destinados a regular en general las materias informáticas. En rigor se trató de una sola iniciativa redactada el año 1986, que fue reelaborada en dos oportunidades el año 1987.

El anteproyecto se inicia con la designación por parte del Ministerio de Justicia Hugo Rosende de una comisión redactora, la cual fue presidida por el abogado Eduardo Hajna. La comisión creada mediante el Decreto Exento N°118, de 15 de septiembre del año 1986, elaboro el anteproyecto en base a cuatro principios fundamentales que fueron los siguientes:

1. La libertad de recolección y transmisión de los datos que genera la actividad externa y social de las personas.
2. Protección de la intimidad, entendida como el atributo que garantiza a toda persona la no divulgación de antecedentes que puedan lesionar su integridad.
3. La facultad de recurrir a los tribunales en demanda del restablecimiento de un derecho conculcado y, por último,

4. La no impunidad de los delitos, en razón de que en los medios informáticos estaría envuelta la fe pública como un valor social¹⁰².

Este anteproyecto nunca llegó efectivamente a discutirse al interior de la Junta de Gobierno¹⁰³.

Luego existieron dos versiones en 1987 del anteproyecto de 1986. La última versión de estas, constaba de 35 artículos divididos en cuatro títulos. Sin embargo, aunque fue el primer intento de proteger los datos personales, se trata de un anteproyecto sin objetivos claramente definidos, que pretendía tratar en un mismo cuerpo legal materias diferenciadas. En cuanto a la protección de datos - que es lo que nos interesa-, el anteproyecto carece de una enumeración adecuada y sistematizada de principios y derechos, y respecto a estos últimos, no se reconoce una categoría de datos especialmente protegidos, como son los datos sensibles. Tampoco se establecen procedimientos especiales para poder ejercer los derechos consagrados ni la creación de una base de datos ni una autoridad de control, omisiones que se consideran esenciales si se pretende proteger eficaz y adecuadamente los datos de carácter personal de las personas.

¹⁰² JIJENA LEIVA, RENATO. 1992. Chile, la protección penal de la intimidad y el delito informático. Santiago de Chile, editorial Jurídica de Chile. P.157-158

¹⁰³ El poder legislativo durante el periodo que va del 11 de marzo de 1981 al 11 de marzo de 1989 lo ejerció la junta de Gobierno, que integraban los Comandantes en Jefe del Ejército, Armada, Fuerza Aérea y el Director General de Carabineros. Sin embargo, como el Comandante en Jefe del Ejército ocupada el cargo de Presidente de la Republica, no integraba la Junta de Gobierno, siendo reemplazado por el oficial de armas del Ejército que le seguía en antigüedad. ANGUITA RAMÍREZ, PEDRO. “La protección de datos personales y el derecho a la vida privada: Régimen jurídico, jurisprudencia y derecho comparado”. op. cit., p.226

4.1.2 Proyectos de ley respecto a la protección de datos personales elaborados luego de 1990

Desde 1990, se han presentado una decena de proyectos de ley vinculados a la protección de la vida privada, la intimidad y los datos personales, donde muy pocas llegaron a convertirse en leyes.

De todas las iniciativas legales, es la Ley N° 19.628, denominada “*Sobre protección de la vida privada*” subtitulada “*Protección de datos de carácter personal*”, la más importante en este sentido y para este trabajo.

Rescatamos y hacemos mención a la existencia de dos proyectos de ley, uno que modifica la Ley N° 19.628 sobre protección a la vida privada y la Ley N° 20.285 sobre acceso a la información pública, y otro que introduce una indicación sustitutiva a los proyectos de ley que modifican la Ley N° 19.628 (Boletines N° 5309-03, 5356-07 y 6298-05). Ambos proyectos se encuentran en suspenso, al interferir el segundo con el primero, y por el segundo no alcanzar el acuerdo necesario entre las fuerzas políticas representadas en el parlamento por lo que se consideró apropiado suspender (también) su tramitación hasta que no se presentaran reformas para promover su aprobación. Juntos hacen sendos avances en materia de reconocimiento de derechos personales y mecanismos de regulación¹⁰⁴.

¹⁰⁴ CELARE. 2011. La Protección de Datos en la Unión Europea y América Latina. [en línea] EUROLAT: Revista de Relaciones Eurolatinoamericanas. Vol. 17 (83)

4.2 Aspectos generales de la protección de datos personales en Chile

La protección de la vida privada tiene consagración legal primeramente en nuestra constitución, específicamente en el artículo 19 N°4 que reconoce el derecho al respeto y protección a la vida privada y pública y a la honra de la persona y su familia, y el N°5 que hace lo mismo al disponer que las comunicaciones y documentos privados solo pueden interceptarse, abrirse o registrarse en los casos y formas determinados por la ley. La esfera de la protección constitucional se sella en el artículo 20 que consagra la acción de protección¹⁰⁵

Como señalamos anteriormente, desde una perspectiva legal, la protección de los datos personales ha tenido principalmente cabida gracias a la Ley N°19.628 “*Sobre protección de la vida privada*”.

<http://eulacfoundation.org/sites/eulacfoundation.org/files/pdf/LA%20PROTECCI%C3%93N%20DE%20DATOS%20EN%20LA%20UE%20Y%20AL.pdf> [consulta: 22 enero 2015]

¹⁰⁵ CHILE. Constitución Política de la Republica.1980, artículo 20: El que por causa de actos u omisiones arbitrarios o ilegales sufra privación, perturbación o amenaza en el legítimo ejercicio de los derechos y garantías establecidos en el artículo 19, números 1°, 2°, 3° inciso cuarto, 4°, 5°, 6°, 9° inciso final, 11°, 12°, 13°, 15°, 16° en lo relativo a la libertad de trabajo y al derecho a su libre elección y libre contratación, y a lo establecido en el inciso cuarto, 19°, 21°, 22°, 23°, 24°, y 25° podrá ocurrir por sí o por cualquiera a su nombre, a la Corte de Apelaciones respectiva, la que adoptará de inmediato las providencias que juzgue necesarias para restablecer el imperio del derecho y asegurar la debida protección del afectado, sin perjuicio d los demás derechos que pueda hacer valer ante la autoridad o los tribunales correspondientes (...).

4.3 Principios que informan la ley chilena de protección de datos personales

Nos referiremos a los principios que han inspirado el articulado de la ley chilena de protección de datos personales, a partir de lo establecidos por la Organización para la Cooperación y el Desarrollo Económico (OCDE)¹⁰⁶ del cual Chile es miembro desde el 11 de enero del 2010, y que deberían irradiar a cualquier normativa futura en esta materia:

- 1. Principio de especificación del propósito o de especificación del fin:** La OCDE establece que *“el propósito de la recogida de datos se deberá especificar a más tardar en el momento que se produce dicha recogida, y su uso se verá limitado al cumplimiento de los objetivos u otros que no sean incompatibles con el propósito original, especificado en cada momento el cambio de objetivo”*.
- 2. Principio de limitación de recogida:** *“Deberán existir límites para la recogida de datos personales y cualquiera de estos datos deberán obtenerse con medios legales y justos y, siempre que sea apropiado, con el conocimiento o consentimiento del sujeto implicado”*.

¹⁰⁶ OECD. Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. [en línea] <<http://www.oecd.org/internet/interneteconomy/15590267.pdf>> [consulta: 15 diciembre 2014]

Como podemos ver, el consentimiento es el elemento esencial que, por regla general, deberá concurrir para que tenga lugar el tratamiento de datos personales.

3. **Principio de calidad de datos:** *“Los datos personales deberán ser relevantes para el propósito de su uso y, en la medida de lo necesario para dicho propósito, exactos, completos y actuales”*.
4. **Regulación de salvaguardias de la seguridad:** *“Se emplearán salvaguardias razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos”*.
5. **Principio de transparencia:** *“Deberá existir una política general sobre transparencia en cuanto a evolución, prácticas y políticas relativas a datos personales. Se deberá contar con medios ágiles para determinar la existencia y la naturaleza de datos personales, el propósito principal para su uso y la identidad y lugar de residencia habitual de quien controla esos datos”*.
6. **Principio de participación individual:** *“Todo individuo tendrá derecho a:*
 - *que el controlador de datos u otra fuente le confirme que tiene datos sobre su persona;*
 - *que se le comuniquen los datos relativos a su persona en un tiempo razonable; a un precio, si existiese, que no sea excesivo; de forma razonable; y de manera inteligible;*

- *que se le expliquen las razones por las que una petición suya según los subapartados (a) y (b) haya sido denegada, así como poder cuestionar tal denegación y;*
- *expresar dudas sobre los datos relativos a su persona y, si su reclamación tiene éxito, conseguir que sus datos se eliminen, rectifiquen, completen o corrijan”.*

7. **Principio de responsabilidad:** *“Sobre todo controlador de datos debe recaer la responsabilidad del cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente” y;*

8. **Protección especial de datos sensibles:** Y aunque no es un principio dentro de estas Directrices de la OCDE, la ley chilena, siguiendo la tendencia del derecho comparado, extendió su protección a una categoría especial de datos personales que se conoce como “datos sensibles”. Aquella información más íntima de la vida de las personas, que en principio, el legislador debe entender que no pueden ser tratados de la misma manera que otros datos personales, sino bajo condiciones determinadas expresamente.

4.4 ¿Qué es un dato personal?

Antes de comenzar a tratar en profundidad este tema, es necesario señalar que es lo que entendemos por Dato Personal.

La palabra dato viene del latín *datum*, *lo que se da*. Y según la Real Academia Española (RAE) su dato es: **1.** m. Antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho; **2.** m. Documento, testimonio, fundamento; **3.** m. *Inform.* Información dispuesta de manera adecuada para su tratamiento por un ordenador.

Podemos ver que el diccionario de la Real Academia Española reconoce la palabra dato como un antecedente, una evidencia sobre algo, una información, que incluso puede ser tratada por un ordenador de manera sistematizada con otros datos. Según la RAE, este dato sirve para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho. Sin embargo, nosotros creemos que un solo dato en sí, no siempre tiene la capacidad para producir tal efecto, ya que, en general, para que este dato pueda proporcionar información sobre una materia o algo determinado, deberá ser tratado o relacionado conjuntamente con otros datos, de manera que considerados todos ellos, permitan proporcionar una información relevante sobre un hecho o algo que se tiene por objeto saber.

La palabra personal viene del latín *personālis*. Y según la RAE su definición es: **1.** adj. Pertenciente o relativo a la persona; **2.** adj. Propio o particular de ella.

A raíz de lo anterior entonces entendemos por dato personal, aquel que dice relación con la persona, el que resulta propio e inseparable de ella y que afecta su vida privada en mayor o menor medida, elevándolo a la calidad de personalísimo, es decir, cuya esfera y ámbito entran exclusivamente en su poder de decisión y disposición. Tal es el caso del nombre, profesión, dirección, edad, nacionalidad, origen racial, situación económica, etcétera.

Buscando una definición legal, las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales¹⁰⁷, definen “datos personales” como cualquier información relacionada con un individuo identificado o identificable (sujeto de datos).

Así también, nuestra legislación recoge este concepto en la Ley N° 19.628, denominada “*Sobre protección de la vida privada*”. Esta define dato personal en el artículo 2 letra f)¹⁰⁸.

Según esta definición, el ámbito de protección de la Ley N° 19.628 protege únicamente los datos personales de las personas naturales. Esta posición ha sido recogida mayoritariamente en fallos de la Corte de Apelaciones de Santiago¹⁰⁹ y de la Corte Suprema¹¹⁰.

¹⁰⁷ OECD. Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. op. cit.

¹⁰⁸ CHILE. Ley 19.628. 1999, artículo 2 letra f): Para los efectos de esta ley se entenderá por: f) Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

¹⁰⁹ Ejemplo de esto es la resolución dictada en causa Rol N°: 5414-2009, por la Corte de Apelaciones de Santiago, donde en su considerando 5° señala: Que en el presente caso, de las citas legales hechas, lo expuesto por las partes y documentos acompañados, resulta que la recurrida se encontraba legalmente facultada para comunicar a la empresa Dicom Interfax la morosidad en que había incurrido la empresa recurrente y que ésta no niega, por tratarse de la deuda de una persona jurídica y no estar por tanto bajo la prohibición tutelar contemplada en la Ley N° 19.628, existiendo además numerosas otras boletas por servicios de la misma clase en estado de morosidad, de tal modo que esta Corte no divisa ilegalidad ni arbitrariedad en el proceder de la recurrida.

¹¹⁰ Ejemplo de esto es la causa n° 4832/2010. Resolución n° 35856, de Corte Suprema de Chile – Sala Tercera (Constitucional), del 24 de Septiembre de 2010. Y donde el considerando 3° señala: De la historia fidedigna de la ley en cuestión es posible desprender de varios pasajes de ésta, sea de la moción, del proyecto original, sus modificaciones y/o discusión en sala, que dicho cuerpo legal se encuentra orientado a la protección de datos personales, entendiendo la noción personal como perteneciente o relativo a la persona natural. Es así como señala en la moción de la ley que: “De acuerdo a la doctrina expresada en los diversos instrumentos internacionales y textos constitucionales que se refieren a la materia, la vida privada de las personas pertenece a la categoría de los derechos humanos”. Agrega más adelante: “Partiendo del precepto contenido en el artículo 19 N° 4 de nuestra Carta Fundamental, nuestra moción comienza anunciando la inviolabilidad de la vida privada y advirtiendo que toda intromisión es, en principio, ilegítima. Se enuncian los principales aspectos a los que ella se extiende, tales como el derecho a la propia imagen; a la intimidad personal y familiar”. Y finalmente se señala en el Primer Informe de la Comisión de Constitución correspondiente al

4.5 Clasificación de los datos personales

Una vez atendido el caso de lo que es un dato personal, cabe preguntarnos ¿Existe un solo tipo de dato personal? ¿tienen todos el mismo valor? ¿será igual de importantes el dato nombre que el dato vida sexual de una persona?. Es lo que trataremos de explicar a continuación.

Si estableciéramos que todos los datos son iguales *per se*, no habría problemas en establecer un mismo ámbito de protección para todos. Esta cuestión podría parecer poco acertada si solo pensamos el efecto que podría producir en nuestra vida privada que alguien sepa que me llamo Juan Romo o Pablo Salinas, en contraposición al hecho de que alguien sepa aspectos de mi vida sexual como cuantas veces tengo relación con mi pareja o si soy heterosexual o homosexual. Parece que desde ese punto de vista, no todo dato es tan importante a la luz de nuestros ojos o de los otros.

Cierto que lo anterior no es compartido por todos a nivel doctrinal, como da cuenta Heredero Higuera al señalar que: “*la doctrina se ha mostrado contraria a definir un tal conjunto de datos, por estimar que los datos, cualesquiera que sean, no son sensibles per se, sino según el contexto en que se usan*”. Sin embargo, también reconoce que tal pensamiento es solo a nivel doctrinal, pues la mayoría de las leyes

segundo trámite constitucional: “Se aclaró que este artículo (artículo 2º) estaba referido a los datos personales de las personas naturales y se aplicaba en el ámbito de la intimidad. Por lo tanto no es aplicable a las personas jurídicas”.

de protección de datos personales si otorga un valor per se a determinados datos, a los que califica de sensibles¹¹¹.

Por lo anterior es que la doctrina ha distinguido tipos de datos en el intento de demostrar que no todos los datos son igual de “sensibles”¹¹²:

1. Datos Personales Públicos: Son aquellos conocidos por un considerable número de personas, sin que el titular de los datos conozca cabalmente cómo fueron difundidos o recogidos, ni que tampoco pueda evitar que una vez conocidos, sigan circulando o comunicándose constantemente.
2. Datos Personales Privados: Son aquellos cuya comunicación se encuentra regulada de manera de impedir su libre difusión, respetando la voluntad de confidencialidad que el titular de los datos quiere imprimirles. Dentro de esta categoría podemos encontrar dos subcategorías:
 - a. Datos íntimos: Son los datos que el titular está obligado a proporcionar regularmente en cumplimiento de sus deberes cívicos.
 - b. Datos secretos: Que son datos muy similares a los datos íntimos, pero que la diferencia radica en que el titular no está obligado a

¹¹¹ HERNANDEZ, ANA. y PALACIOS, JUAN. 2008. El dato sensible: su tratamiento en Chile y en el derecho comparado. Memoria de prueba para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile, Facultad de Derecho. p.80

¹¹² El tema del dato sensible no será tratado en este trabajo de manera profunda, basta saber que no todos los datos tienen el mismo grado de importancia, y que así lo demuestran los proyectos y leyes respecto a la protección de datos. Basta enunciar la Ley N° 19.628 “*Sobre protección de la vida privada*”, que en su artículo 2 literal g) define el dato sensible.

proporcionarlos a alguien, salvo que medie un caso excepcional regulado expresamente por la ley. A su vez, estos últimos se pueden dividir en: i) datos profundos y; ii) datos reservados, atendiendo a si el dato puede o no darse a conocer. Justamente, se entiende que el dato reservado es aquel en que su titular no está obligado a darlo a conocer, bajo ningún motivo, a menos claro que medie su voluntad, a diferencia del dato profundo que, si bien en principio el titular no está obligado a entregarlo, admite excepciones¹¹³. *R. Nerson considera que el hombre no puede aislarse constantemente en una “torre de marfil”, pues vive en una sociedad, por lo que con las comunicaciones que se establecen se da la ocasión para que secretos de orden íntimo puedan ser conocidos. Lo que la ley ha de evitar, principalmente, es la investigación o fisgoneo indiscreto de informaciones concernientes a la personalidad ajena*¹¹⁴

Victor Drumond¹¹⁵ divide los datos en:

1. Datos cuyo tratamiento es prohibido: Son los datos que dicen relación con los hábitos de vida, la intimidad del ámbito privado familiar.
2. Datos sensibles: Tales como las convicciones filosóficas, origen racial, fe religiosa, salud, etcétera.

¹¹³ HERNANDEZ, ANA. y PALACIOS, JUAN. “El dato sensible: su tratamiento en Chile y en el derecho comparado”. op. cit. p.80

¹¹⁴ NOVOA MONREAL, EDUARDO. “Derecho a la vida privada y la libertad de información: Un conflicto de derechos”. op. cit., p.52

¹¹⁵ DRUMMOND, VÍCTOR. “Internet, Privacidad y Datos personales”. op. cit., p.51 y sgtes.

3. Datos no sensibles: Aquellos cuyo tratamiento se efectúe con mayor facilidad, tales como el nombre, apellido, fecha de nacimiento, sexo, etcétera. Estos datos según el autor, no provocan en sí mismos una sustantiva relevancia en la privacidad del titular.

De esta forma, podemos ver como la doctrina se preocupa de hacer una diferenciación en torno al dato y su valor, denotando la importancia que tienen algunos datos personales sobre otros, y por lo tanto, la necesidad que aquellos datos que parecen más “sensibles” sean objetos de una protección mayor por parte de la ley.

Así también, la legislación en nuestro país, realiza una clasificación de los datos personales, en el artículo 2 de la Ley 19.628, que veremos más adelante en este mismo capítulo.

4.6 Protección constitucional

Desde la Constitución Política de la República del año 1925, se consagra como derecho fundamental la protección a los ciudadanos de injerencias ilegítimas en su ámbito personal, protegiendo la inviolabilidad del hogar, la correspondencia y sobre cierto tipo de comunicación privada¹¹⁶, haciendo muy acotado y específico el ámbito

¹¹⁶ CHILE. Constitución Política de la República. 1925, artículo 10: Asimismo, la Constitución asegura a todos los habitantes de la República: 12°.- La inviolabilidad del hogar. La casa de toda persona que habite el territorio chileno sólo puede ser allanada por un motivo especial determinado por la ley, y en virtud de orden de autoridad competente;

de protección a la vida privada. Lo más rescatable de esta norma para la época, es que ya se comenzaba a entender un cierto tipo de relación entre la intimidad con la protección del hogar, en cuanto a crear en él, un ámbito libre de intromisión de terceros.

Como señalamos al principio de este capítulo, es la Constitución Política de la República de 1980 vigente actualmente, la que incorpora de manera expresa la protección constitucional de la vida privada en sus artículos 19 n°4, y extendiendo esta protección al hogar de la persona en el artículo 19 n°5¹¹⁷.

Sin embargo, y como vimos en el primer capítulo, nuestro sistema normativo no define lo que debe entenderse por “vida privada”, ni tampoco señala el contenido de su ámbito de protección de este derecho. Es más, en el mismo artículo se protege tanto la vida privada como la honra, dos derechos distintos¹¹⁸, lo que solo sirve para confundir más este discutido concepto¹¹⁹.

13.- La inviolabilidad de la correspondencia epistolar y telegráfica y de las comunicaciones telefónicas. No podrán abrirse, ni interceptarse, ni registrarse los papeles o efectos públicos, sino en los casos expresamente señalados por la ley.

¹¹⁷ CHILE. Constitución Política de la República. 1980, artículo 19 n°4 y n°5: La Constitución asegura a todas las personas: 4°.- El respeto y protección a la vida privada y a la honra de la persona y su familia; 5°.- La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley.

¹¹⁸ Asimismo lo sostuvo la propia Comisión de Estudio de la Nueva Constitución, donde concretamente intervino el prof. Guzman, al señalar que “vida privada” y “honra”, eran dos conceptos y derechos distintos al decir que “estima que el primer valor que debe consagrarse en este precepto, es el derecho a la privacidad. El segundo es el derecho a la honra”. GUZMÁN ERRAZURIZ, JAIME. Actas oficiales de la comisión constituyente. Tomo IV (129), 12 de junio de 1975. p.337

¹¹⁹ Respecto a este punto, ver capítulo I en cuanto intentamos explicar que se entiende por vida privada o privacidad y algunas de las principales teorías que buscan responder cual es el contenido y ámbito de protección de este derecho.

Así, aunque no existe una referencia expresa a “datos personales” en nuestra Constitución, estos se entienden quedarían protegidos en el derecho a la vida privada del 19nº4, y de manera específica a cierto ámbito de protección en el 19nº5, pues, como vimos en el punto 4.4 la Ley 19.628 en su artículo 2 letra f) define dato personal como *“los relativos a cualquier información concerniente a personas naturales, identificadas o identificables”*.

4.7 Análisis de la Ley N° 19.628 “Sobre protección de la vida privada”

4.7.1 Generalidades

En términos generales, la Ley N°19.628 ha intentado recoger las experiencias y avances obtenidos en las legislaciones contemporáneas sobre esta materia, y sobre todo las formas y modos que la doctrina ha encontrado para proteger de mejor manera la privacidad del individuo en cuanto a sus datos personales.

Como señala Rodrigo Álvarez en su tesis *“Por medio de la Ley N° 19.628 se entregan los medios e instrumentos a través de los cuales los individuos pueden proteger eficientemente la utilización no consentida por su titular y por terceros extraños, de sus datos personales susceptibles de un tratamiento automatizado, de modo que a su respecto se confecciona un tipo de información de carácter informático, o más bien*

dicho, se le otorga una identidad informática, que puede llevarle a afectar todo su entorno, ya sea, social, profesional o personal”¹²⁰.

4.7.2 Ámbito de aplicación

La Ley N° 19.628 tiene como objeto principal la regulación o protección de los bancos de datos en general sea en formato análogo o digital y no específicamente para el caso de Internet ni su uso por la telefonía móvil, sin embargo, esto no quita que lo dispuesto por esta norma le sea totalmente aplicable en lo que corresponde a la telefonía móvil como veremos

Toda información que genera, se recoge y se envía a través de un móvil, tiene como destino una base de datos digital¹²¹. De hecho el celular como un computador, genera bases de datos de nuestra información en su memoria interna o una memoria externa que en general son memorias micro SD¹²². Todo lo que hacemos en nuestro celular es respaldado en nuestra memoria, y muchas veces en un servidor¹²³ externo

¹²⁰ ÁLVAREZ, RODRIGO. 2002. Análisis del régimen jurídico de protección de datos de carácter personal. Memoria de prueba para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile, Facultad de Derecho. p.92

¹²¹ En este caso una base de datos se entenderá, como un conjunto de datos de un mismo contexto, organizados sistemáticamente en un ordenador o servidor, de manera que un programa dentro de él pueda seleccionar rápidamente aquellos datos o fragmentos que necesite.

¹²² SD (Secure Digital). Micro SD es un formato de memoria de tarjeta flash de pequeñas dimensiones (Mide tan solo 15 × 11 × 1 milímetros, lo cual le da un área de 165 mm²) de gran capacidad digital, pero con tasas de transferencia no muy altas (un archivo puede demorarse más en ser ejecutado). Su pequeño tamaño permite maximizar rendimiento, comodidad y eficacia, lo que las hace ideal a aplicaciones donde el tamaño es crítico, como los teléfonos móviles, sistemas GPS o tarjetas Flash para consolas de mano.

¹²³ “Un servidor, como la misma palabra indica, es un ordenador o máquina informática que está al “servicio” de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a estos, todo tipo de información. A

a él, como en el caso de cada llamada telefónica que realizamos, ya que, estas llamadas son almacenada en los servidores del proveedor de telefonía celular, de esta manera nuestro proveedor sabe a quién, cuanto y cuando marcamos un número.

Con respecto al titular de los derechos que la Ley N° 19.628 protege debemos remitirnos a su artículo 2 letra f), que como vimos señala: “*Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables*”. De aquí se desprende entonces, que sus disposiciones dejan fuera del ámbito de aplicación a las personas jurídicas, preocupándose solamente de las personas naturales¹²⁴. A la misma conclusión llegamos al leer la letra ñ) del mismo artículo¹²⁵

Parece claro que la vida privada es un derecho exclusivo de las personas naturales, aunque, no parece inconveniente para que le fuera otorgada a las personas jurídicas. Tal conclusión se desprende de la amplia interpretación que tanto la doctrina como la jurisprudencia le han dado al término “persona”, derivado de la

modo de ejemplo, imaginemos que estamos en nuestra casa, y tenemos una despensa. Pues bien a la hora de comer necesitamos unos ingredientes por lo cual vamos a la despensa, los cogemos y nos lo llevamos a la cocina para cocinarlos. Así en nuestro ejemplo, nuestra máquina servidor sería la despensa, y los clientes somos nosotros como personas que necesitamos unos ingredientes del servidor o despensa. Pues bien con este ejemplo podemos entender ahora un poco mejor qué es un servidor. Por tanto un servidor en informática será un ordenador u otro tipo de dispositivo que suministra una información requerida por unos clientes (que pueden ser personas, o también pueden ser otros dispositivos como ordenadores, móviles, impresoras, etc.)”. APRENDERAPROGRAMAR. Qué Es Un Servidor y Cuáles Son Los Principales Tipos De Servidores (proxy, Dns, Web, Ftp, Smtplib...). [en línea] <http://www.aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftpsmtplib&catid=57:herramientas-informaticas&Itemid=179> [consulta: 09 septiembre 2014].

¹²⁴ El proyecto original de la ley de protección de datos de carácter persona, en un principio, confería los derechos de la ley no solo a las personas naturales, sino que también a las jurídicas y a las morales. Pero luego de pasar por el Senado, quedo en su forma actual, restringida exclusivamente a las personas naturales.

¹²⁵ Para los efectos de esta ley se entenderá por: ñ) Titular de los datos, la persona natural a la que se refieren los datos de carácter personal.

primera parte del artículo 19 de la Constitución. Además hay otras normas que establecerían categorías de secreto distintas de la ley estudiada, como es el caso del secreto bancario, que no ha hecho distinción alguna entre personas naturales y personas jurídicas.

Respecto a la protección de datos personales, deberá entenderse que para la información de datos de personas jurídicas no serán aplicables los principios de privacidad, ni la prescripción de datos del artículo 18¹²⁶ de esta ley, situación que si podría haberse estimado protegida por nuestra Constitución.

“Como una posibilidad diferente Hernán Corral sostiene que la privacidad tiene como sujeto a la familia, lo que efectivamente fluye del propio texto de la Constitución que asegura “el respeto y la protección a la vida privada y pública y a la honra de la persona y su familia”. Sin embargo, para efectos de la presente ley, sería impropio hablar de la familia como titular de datos, por la propia definición que ella otorga, y por tratarse de datos de carácter personal, más que familiar”¹²⁷.

¹²⁶ “En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible.

Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de haber sido pagada o haberse extinguido por otro modo legal (...)”

¹²⁷ ÁLVAREZ, RODRIGO. “Análisis del régimen jurídico de protección de datos de carácter personal”. op. cit., p.97

4.7.3 Objetivos

En su tesis, Rodrigo Álvarez a través de la historia fidedigna de la ley y sus disposiciones identifica los siguientes objetivos¹²⁸:

- Proporcionar una normativa específica que proteja eficazmente a los individuos frente a las nuevas formas de ataque a la intimidad, en una sociedad tecnológicamente avanzada.

Como señalamos, antes de esta ley no existía en Chile una norma de estas características, si había proyectos que no llegaron a concretarse. Los conflictos de interés que con motivo del conflicto de datos personales se presentaren, encontraban solución en forma exclusiva en la Constitución, lo que a la postre entregaba un gran poder de discrecionalidad a los jueces, que no tenían una ley especial que regulara esta materia.

Lo que se buscó por los legisladores con la creación de una ley con estas características fue la de otorgar una protección de carácter jurídico al individuo, frente a una amenaza informática, evitando con ello la utilización por terceros extraños y no consentida por el titular, de sus datos susceptibles de tratamiento automatizado.

¹²⁸ *Ibíd.*, p.97-99

- Establecer un sistema que permita controlar a los bancos de datos.

Para que un sistema de protección de banco de datos sea confiable y eficaz, es necesario el establecimiento de un ajustado sistema de control sobre él. Es por esto que uno de los objetivos principales de la ley, fue la de otorgar un control de carácter individual, ejercido por el propio individuo que es titular de los datos, sobre la información que a su respecto circula y que se instrumentaliza principalmente, en el llamado derecho de acceso¹²⁹. Así también, se establece un control institucional, ya sea en el ámbito jurisdiccional como administrativo. Así es, como la Ley N° 19.628, ha establecido un procedimiento de reclamo ante el Juez de letras en lo Civil, con el propósito de que el titular de los datos solicite amparo a los derechos consagrados en la Ley¹³⁰. Además, ha ordenado que, el Servicio de Registro Civil e Identificación lleve una nómina de los banco de datos personas a cargo de organismos públicos.

- Lograr un equilibrio entre el derecho a la intimidad que consagra el artículo 19 N° 4 de la Constitución Política de la Republica y el derecho a la información fundado en razones de Orden Público.

Es innegable que, tanto el Estado como a los particulares, no se les puede despojar de su legítimo interés en contar, el primero, con mecanismos más eficientes para dar cumplimiento a sus fines, y a los segundos, del derecho a desarrollar una actividad lícita. Es por esta razón, que la ley da a las personas los mecanismos y herramientas

¹²⁹ Que es la facultad que tiene de conocer e informarse sobre los datos relativos a su persona, su procedencia y destinatario, sobre el propósito de su almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente. ÁLVAREZ, RODRIGO. “Análisis del régimen jurídico de protección de datos de carácter personal”. op. cit., p.98

¹³⁰ Título II, artículo 12 y siguientes de la Ley N° 19.628.

necesarias que permitan controlar sus datos personales, reconociendo expresamente el principio de libertad de iniciativa en la recolección, procesamiento y eventual transmisión de información personal de los individuos, siempre que se haga de una manera coincidente con la propia ley y con las finalidades permitidas por el ordenamiento jurídico.

4.7.4 Estructura

La ley sobre Protección de la Vida Privada se estructura a través de ocho partes, en un total de 24 artículos y 3 artículos transitorios, enfocados a la protección de los datos personales como veremos a continuación:

- 1. Título Preliminar “Disposiciones generales”**, comprende los artículos 1 al 3. El artículo 2 es particularmente importante, pues, define una serie de conceptos vitales para el cabal entendimiento de esta ley, como son: “almacenamiento de datos”, “datos personales”, “datos sensibles”, “banco de datos”, etcétera.
- 2. Título I “De la utilización de datos personales”**, que va desde el artículo 4 al 11. El artículo 4 establece la importancia de la ley y del consentimiento de la persona en el tratamiento de datos.

3. **Título II “De los derechos de los titulares de datos”**, que comprende los artículos 12 al 16. Este título es medular en cuanto a los derechos que tienen los particulares en cuanto a poder requerir a los responsables del registro de banco de datos, información, modificación o eliminación de sus datos, así también contando con un procedimiento ante el juez de letras en lo civil o la corte suprema en caso de negativa al requerimiento de ellos.
4. **Título III “De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial”**, comprendiéndolos artículos 17 al 19.
5. **Título IV “Del tratamiento de datos por los organismos públicos”**, materia que tratan los artículos 20 a 22.
6. **Título V “De la responsabilidad por las infracciones a esta ley”**, que consta solo del artículo 23.
7. **Título Final**, que comprende solo el artículo 24.
8. **Disposiciones Transitorias**, el que consta de tres artículos.

4.7.5 Tipos de datos consagrados

Como señalamos, junto con establecer una reglamentación relativa al tratamiento y a la protección de los datos personales, la ley ha fijado en su artículo segundo una serie de conceptos vitales para entender la ley, y las diversas figuras que a través de ella se han creado. Lo anterior responde a la necesidad de que frente a aspectos tan técnicos como la informática, se busque un marco teórico a través del cual se permita una correcta interpretación de sus preceptos, y una correcta aplicación de la ley. A esto responde la creación de un glosario técnico, solución a la que también han llegado las legislaciones europeas y americanas en esta materia.

De esta manera, podemos apreciar la siguiente clasificación:

- a) **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.

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

c) Datos de carácter personal como tal o datos personales: los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

La redacción de este concepto da una gran amplitud interpretativa a los Tribunales encargados de aplicar esta ley, ya que, otorga la posibilidad de no cerrar la inclusión de datos personales protegidos.

La actual redacción es claramente distinta y práctica, que la que el proyecto de ley consagraba hacia septiembre de 1997, cuando se entendía que “*Datos de carácter personal, son los relativos a cualquier información concerniente a personas físicas, identificadas o identificables, que denoten alguna característica física o de su personalidad, o que se refieran a hechos o circunstancias de su vida privada, intimidad o a información de carácter sensible, tales como el origen racial o étnico, las opiniones políticas, las convicciones religiosas y filosóficas, la pertenencia a sindicatos, la salud o la sexualidad*”¹³¹. Mientras que por datos sensibles incluía además “*los datos relativos a hábitos personales, estados de salud físicos o psíquicos, enfermedades y las condenas criminales*”¹³².

Como podemos ver, la amplitud del concepto de dato personal, hacia inútil la existencia de un concepto estricto de dato sensible. No obstante, las posteriores discusiones producidas en la comisión mixta dieron a la luz el concepto que finalmente concluyó por ser el definitivo de la ley, dando lugar a la existencia de

¹³¹ Historia de la Ley 19.628, p. 141.

¹³² *Ibíd.*

la institución jurídica de los datos sensibles con absoluta prescindencia del concepto detallista de dato personal que hacia el año 1997 se había establecido¹³³.

d) 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.

Por ende, de lo anterior podemos señalar las siguientes categorías de datos sensibles: i) Hábitos personales; ii) origen racial; iii) ideologías y opiniones políticas; iv) creencias o convicciones religiosas; v) Estados de salud físicos o psíquicos y; vi) la vida sexual.

El concepto de dato sensible fue incorporado al proyecto de ley el año 1997 en el “segundo informe de la comisión de constitución, legislación y justicia”, junto con la redacción de los demás literales del artículo segundo. Con anterioridad a esa fecha sólo existía en el proyecto original, el concepto de datos personales. La redacción original es similar a la que existe hoy en día: *“Dato sensible, los datos personales que se refieren a las características físicas o morales de las personas, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las*

¹³³ HERNANDEZ, ANA. y PALACIOS, JUAN. “El dato sensible: su tratamiento en Chile y en el derecho comparado”. op. cit. p.182

creencias o convicciones religiosas, los estados de salud físicos o psíquicos, las enfermedades, la vida sexual y las condenas criminales”¹³⁴.

4.7.6 Requisitos para realizar un tratamiento de datos

La Ley N° 19.628 establece en el inciso segundo del artículo 1° y el artículo 4 que toda persona puede efectuar un tratamiento de datos personales sujeta, empero, al cumplimiento de ciertos requisitos:

1. Que se encuentre autorizado por la ley, por otras disposiciones legales, o por el titular de datos personales mediante su consentimiento. Sin embargo, en ciertos casos determinados en el inciso quinto y sexto, los datos pueden ser procesados sin que medie la autorización del titular.
2. Que la finalidad del tratamiento se encuentre permitida por el ordenamiento jurídico.
3. Que se respeten las facultades que la ley concede a los titulares de los datos personales.

¹³⁴ HERNANDEZ, ANA. y PALACIOS, JUAN. “El dato sensible: su tratamiento en Chile y en el derecho comparado”. op. cit. p.183-184

4. Que se respete el pleno ejercicio de los derechos fundamentales de los titulares de los datos personales.

4.7.7 Sujetos que participan en el tratamiento de datos personales

Los sujetos que participan en esta relación que se da en torno al tratamiento de datos básicamente son dos:

- a) El titular de datos;
- b) El responsable del registro de banco de datos y;
- c) Cesionario

4.7.7.1 El titular de datos

Como vimos la letra ñ) del artículo 2 define al titular de datos como la persona natural a la que se refieren los datos de carácter personal.

Explicamos que la ley se refiere solo a las personas naturales y excluye de esta categoría a las personas jurídicas¹³⁵.

¹³⁵ Han existido iniciativas legales que han pretendido incorporar a esta definición a este tipo de personas. Un ejemplo de ellos es el Boletín 2422-07 que “*Establece normas sobre protección de la información de las personas jurídicas*”.

4.7.7.2 El responsable del registro de banco de datos

La letra n) del artículo 2 define al responsable del registro de banco de datos¹³⁶, y se refiere a él el artículo 5 que lo faculta para establecer un procedimiento automatizado de datos personales. También el artículo 6 que establece que sobre el responsable pesa la obligación de eliminar, modificar o bloquear datos personales sin requerimiento del titular. El artículo 11 le impone a esta persona el deber de cuidar los registros o bases de datos con la debida diligencia debiendo responder (de culpa leve) por los daño producidos; el artículo 12 que lo señala como la persona ante quien se ejerce el derecho de acceso o *Habeas Data*. El artículo 16 que señala que su domicilio determina la competencia de los tribunales y, el artículo 17 que establece que en ciertos casos, lo faculta para comunicar a terceros datos patrimoniales negativos.

Una de las grandes críticas que recibe la Ley N° 19.628 es que ella contempla la obligación de los responsables de inscribirse en un registro, únicamente a los responsable del sector público, lo que genera en consecuencia que la mayoría de las personas ignoren que otros están tratando sus datos personales, y lo que es peor,

¹³⁶ Para los efectos de esta ley se entenderá por: n) Responsable del registro o banco de datos, la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal.

desconocen contra quién deben accionar en el evento de sufrir un perjuicio por el mal manejo.

4.7.7.3 Cesionarios

Admite la ley además del titular y el responsable del tratamiento de datos personales, la intervención de terceras personas, aquellas a los que se les comunican o transfieren los datos de conformidad a lo que establece el artículo 5 de la ley “*El responsable del registro o banco de datos personales podrá establecer un procedimiento automatizado de transmisión (...)*”.

Finalmente, también es posible que intervengan mandatarios encargados del tratamiento de datos personales, como lo establece el inciso primero del artículo 8. En ese caso el mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos. A este mandato se le aplicaran las reglas generales, y deberá respetar las estipulaciones hechas en cumplimiento de su encargo.

4.7.8 Derechos de los titulares de datos personales¹³⁷

¹³⁷ ANGUIITA RAMÍREZ, PEDRO. “La protección de datos personales y el derecho a la vida privada: Régimen jurídico, jurisprudencia y derecho comparado”. op. cit., p.306-313

Como mencionamos cuando vimos la estructura de la Ley N° 19.628, el título II establece los derechos de los titulares de datos. En él los artículos 12 al 15 indican cuáles son los derechos subjetivos que se confiere a los titulares de datos (derecho de información, acceso, modificación, eliminación o cancelación, bloqueo), y el artículo 16 reglamenta la acción mediante la cual se busca asegurar la tutela jurídica de estos derechos. Asimismo, la ley contempla otros derechos, como el derecho a conocer la comunicación de los datos, oposición e indemnización.

4.7.8.1 Derecho de información en la recogida de datos

La Ley N° 19.628 no confirió un derecho general a los titulares de ser informados de modo expreso, preciso e inequívoco, previo a la recogida de datos personales, de un conjunto mínimo de antecedentes como si se hace en el derecho comparado¹³⁸. Sin embargo, la ley si consagró un derecho de información limitado cuando se trata de la recolección de datos personales efectuada por encuestas, estudios de mercado, sondeos de opinión u otros instrumentos semejantes, en cuyo caso debe informarse al interesado sobre el carácter obligatorio o facultativo de las

¹³⁸ En España, el artículo 5 de la Ley Organica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal concede el derecho al interesado, previo a la recogida de datos, de exigir la siguiente información:

- a) Existencia del fichero al que van a ser incorporados los datos, finalidad del mismo y destinatario de los datos.
- b) Carácter voluntario u obligatorio de su respuesta a las preguntas que planteen en relación con sus datos.
- c) Consecuencias de proporcionar los datos o de negarse a ello.
- d) Posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición
- e) Identidad y dirección del responsable del fichero o su representante

La norma exime del deber de suministrar la información descrita en los puntos b), c) y d) en los casos que dicha información se desprenda de la naturaleza de los datos personales que se requieren o de las circunstancias en que se recaban.

respuestas y el propósito para el cual se requiere la información. La ley también impone el deber de omitir las señas que puedan permitir la identificación de las personas consultadas¹³⁹.

4.7.8.2 Derecho de acceso

Consiste en el derecho que tiene el titular de los datos personales da obtener gratuitamente información:

- Sobre datos relativos a su persona;
- su procedencia y destinatario;
- el propósito del almacenamiento y;
- la individualización de las personas u organismos a los cuales sus datos son o serán transmitidos regularmente

El titular, previa solicitud, puede requerir copia autorizada del registro al responsable de la base de datos. El derecho a obtener copia gratuita sólo se puede ejercer personalmente. En caso de que los datos estén en una base de datos a la cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de estos. El derecho de acceso del titular a sus datos personales no puede ser limitado por medio de ningún acto o convención. Existen causales por las cuales puede denegarse el acceso a los datos personales que son: 1) Cuando impida o entorpezca

¹³⁹ Ley N° 19.628, inciso primero, artículo 3.

el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o 2) afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la nación o el interés nacional.

4.7.8.3 Derecho de modificación¹⁴⁰

La ley denomina derecho de modificación a la facultad que tiene el titular para alterar un registro de un banco de datos.

Dice el inciso segundo del artículo 12 de la ley, que el titular de los datos personales tiene la facultad de requerir al responsable del tratamiento de datos la modificación de los mismos en caso que, y estos son los supuestos que lo permiten, se encuentren erróneos, inexactos, equívocos o incompletos, lo que deberá acreditar. La ley en el artículo 2 letra j) entiende por modificación de datos *“todo cambio en el contenido de los datos almacenados en registros o bancos de datos”*.

El ejercicio de este derecho, al igual que el derecho de acceso es gratuito. El titular previa solicitud puede requerir copia al responsable de la base de datos del registro alterado en la parte pertinente. El derecho a obtener copia gratuita solo se puede ejercer personalmente. En caso de efectuarse nuevas modificaciones, podrá pedir copia gratuita del registro actualizado, siempre que hayan pasado 6 meses

¹⁴⁰ El profesor Pedro Anguita Ramírez señala que, en el derecho comparado la facultad conferida al titular de los datos para solicitar la modificación de sus datos personales suele denominarse Derecho de Rectificación. ANGUIITA RAMÍREZ, PEDRO. “La protección de datos personales y el derecho a la vida privada: Régimen jurídico, jurisprudencia y derecho comparado”. op. cit., p.308

desde la última vez que ejerció este derecho, en caso contrario, deberá cancelar la tarifa fijada por el responsable de la base de datos.

El derecho del titular a solicitar la modificación de sus datos personales no puede ser limitado por medio de ningún acto o convención.

La ley en los casos en que proceda le impondrá la obligación al responsable de la base de datos de modificar los datos sin necesidad de que lo requiera al titular.

La ley también establece las causales por el cual el responsable puede denegar la modificación de los datos personales cuando: 1) impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido o, 2) afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la nación o el interés nacional, y 3) por último, tampoco se podrá pedir la modificación de los datos personales almacenados por mandato legal fuera de los casos contemplados en la ley respectiva.

4.7.8.4 Derecho de eliminación o cancelación

La Ley N° 19.628 utiliza los términos eliminación y cancelación como sinónimos al definir ambas operaciones bajo el mismo numeral como “...*la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello*”¹⁴¹.

¹⁴¹ Ley N° 19.628, artículo 2, letra h) .

Este derecho puede ejercitarse en caso que el almacenamiento carezca de fundamento legal, cuando los datos estuvieren caducos¹⁴² o si se proporcionaron voluntariamente y se usan para comunicaciones comerciales y no desea continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

El ejercicio de este derecho, al igual que los derechos de acceso y de modificación, es gratuito. El titular previa solicitud puede requerir copia al responsable de la base de datos del registro alterado en la parte pertinente. El derecho a obtener copia gratuita solo se puede ejercer personalmente.

El derecho del titular a solicitar la modificación de sus datos personales no puede ser limitado por medio de ningún acto o convención.

La ley en los casos en que proceda le impondrá la obligación al responsable de la base de datos de modificar los datos sin necesidad de que lo requiera al titular.

Las causales para denegar la eliminación de datos personales son las mismas que puede invocar el responsable de las bases de datos para desestimar el acceso y la modificación de los mismos, es decir, cuando: 1) impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido o, 2) afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la nación o el interés nacional¹⁴³, y 3) por último, respecto de datos

¹⁴² Ley N° 19.628, artículo 2, letra h), en relación con el artículo 6, inciso primero, y artículo 12, inciso tercero.

¹⁴³ Ley N° 19.628, artículo 15, inciso primero.

personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva¹⁴⁴.

4.7.8.5 Derecho de bloqueo

La ley define el bloqueo de datos como “*la supresión temporal de cualquiera de las operaciones del tratamiento de los datos almacenados*”¹⁴⁵. Consiste en la facultad que tiene el titular de los datos personales para exigir que se suspenda temporalmente el tratamiento de datos almacenados, cuando respecto de ellos no corresponda cancelación

A través de este derecho, el titular persigue que se suspenda cualquier operación o conjunto de operaciones o procedimiento técnicos destinados a utilizar sus datos de cualquier forma.

Hay que señalar que el ejercicio de este derecho, supone que el titular haya proporcionado sus datos voluntariamente.

En materia de comunicaciones comerciales y marketing directo, se legalizó el envío de correos electrónicos no solicitados permitiéndose a los titulares de datos personales ejercer el derecho de bloqueo en su modalidad de Opt.-out, así de esta

¹⁴⁴ Ley N° 19.628, artículo 15, inciso segundo.

¹⁴⁵ Ley N° 19.628, artículo 2, letra b)

manera, el responsable del banco de datos no podrá continuar enviando comunicaciones comerciales y correos electrónicos no solicitados a quien ha ejercido este derecho.

El ejercicio de este derecho, al igual que los derechos de acceso, modificación y eliminación, es gratuito.

El derecho del titular a solicitar el bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención.

La ley en los casos en que proceda le impondrá la obligación al responsable de la base de datos de bloquearlos sin necesidad de que lo requiera al titular¹⁴⁶. Las causales para denegar el bloqueo de datos personales son las mismas que puede invocar el responsable de las bases de datos para desestimar el acceso, modificación y cancelación de los mismos, y que son: 1) impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido o; 2) afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la nación o el interés nacional¹⁴⁷ y; 3) respecto de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva¹⁴⁸.

¹⁴⁶ Ley N° 19.628, artículo 6, inciso cuarto.

¹⁴⁷ Ley N° 19.628, artículo 15, inciso primero.

¹⁴⁸ Ley N° 19.628, artículo 15, inciso segundo.

4.7.8.6 Derecho a conocer la comunicación de los datos

El titular de la información tiene la facultad de exigir al responsable de la base de datos la individualización de las personas u organismos a los cuales sus datos se transmiten regularmente¹⁴⁹. De este mismo modo, si se hubiese comunicado a personas determinadas o determinables datos personales que estuvieren cancelados o modificados, el responsable de la base de datos deberá notificarle, avisarles, a la brevedad posible la operación efectuada. En los casos que no fuere posible determinar a las personas a quienes se les haya comunicado, el responsable, dice la ley, deberá poner aviso de general conocimiento para quienes usen la información de la base de datos¹⁵⁰

4.7.8.7 Derecho de oposición

El derecho de oposición solo se consagra en un caso específico de la Ley N° 19.628, y este se encuentra en el artículo 3, inciso segundo que dispone que “*el titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión*”.

¹⁴⁹ Ley N° 19.628, artículo 12, inciso primero.

¹⁵⁰ Ley N° 19.628, artículo 12, inciso sexto.

4.7.8.8 Derecho a indemnización

Aunque la Ley N° 19.628 no consagra este como un derecho, sino como un deber del responsable de la base de datos, el titular tiene derecho a ser indemnizado por los daños patrimoniales y morales sufridos a consecuencia de un tratamiento indebido de sus datos personales. El ejercicio de este derecho es compatible con los derechos de eliminación, modificación o bloqueo de los datos personales que efectuó el titular¹⁵¹.

La ley en su artículo 23, inciso segundo y tercero, establece un conjunto de reglas especiales respecto del ejercicio de la acción de indemnización de perjuicios. El afectado por un tratamiento indebido de sus datos tiene tres alternativas: 1) deducir únicamente la acción de indemnización de perjuicios, sin que el titular de los datos personales ejerza la acción de reclamación, la cual se rige por el procedimiento sumario; 2) ejercer la acción de indemnización de perjuicios junto a la acción de reclamación, que persigue establecer una infracción a la ley, lo cual es compatible con la solicitud de eliminación, modificación o bloqueo de sus datos. El ejercicio de la acción resarcitoria se rige también por el procedimiento sumario, al igual que las infracciones no contempladas en los artículos 16 y 19 de la Ley N° 19.628; 3) deducir una demanda de indemnización de perjuicios, la cual se sujetara a las normas de

¹⁵¹ Ley N° 19.628, artículo 23, inciso primero.

responsabilidad extracontractual del libro IV del Código Civil, de acuerdo al procedimiento ordinario contemplado en el Código de Procedimiento Civil.

4.7.9 Obligaciones del responsable del tratamiento de datos personales

La Ley N° 19.628 exigió escasas obligaciones a las personas dedicadas a tratar datos personales, de ahí muchas de sus críticas. No dispuso de un deber general, sino solo se le impuso al responsable de los registros o bases de datos donde se almacenen datos personales con posterioridad a su recolección, la obligación de cuidarlos con la debida diligencia, asignándole la responsabilidad por los daños que se causen¹⁵². La ley, tampoco le ordena al responsable la obligación de comunicar la creación de una base de datos privada a algún ente público como vimos, ni los cambios que incidan en su finalidad, persona del responsable o ubicación física de este último. El único deber que reconocemos en cuanto a los responsables de los registros o bases de datos donde se almacenen datos personales, es el que recae sobre los organismos públicos, cuyos responsables tienen el deber de notificar al Servicio de Registro Civil e Identificación¹⁵³, según las reglas que a continuación explicaremos¹⁵⁴:

¹⁵² El profesor Pedro Anguita Ramírez explica que a nivel comparado tanto el derecho comunitario como los países de la Unión Europea que traspusieron la Directiva 95/46 sobre protección de datos personales ordenan a los responsables de bases de datos la adopción de medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos, de forma de evitar su alteración, pérdida, tratamiento o acceso no autorizado. Las medidas de seguridad se adoptan en función de la naturaleza de los datos almacenados y los riesgos humanos o naturales a que estén expuestos. ANGUITA RAMÍREZ, PEDRO. “La protección de datos personales y el derecho a la vida privada: Régimen jurídico, jurisprudencia y derecho comparado”. op. cit., p.314

¹⁵³ Ley N° 19.628, artículo 22, inciso primero.

¹⁵⁴ Ley N° 19.628, artículo 22, inciso segundo y tercero.

- i. El fundamento jurídico de su existencia.
- ii. Su finalidad.
- iii. El tipo de datos almacenados en la base de datos y;
- iv. La descripción del universo de personas que comprende esta base de datos.

La Ley N° 19.628 remite a una disposición reglamentaria la definición de los términos de la notificación y registro¹⁵⁵.

Por ultimo podemos decir que, el responsable de las bases de datos a cargo de organismos públicos debe notificar cualquier cambio en los puntos descritos precedentemente en el plazo de 15 días desde que se produzcan¹⁵⁶.

4.7.10 Acciones que contempla la ley

La Ley N° 19.628 contempla dos acciones de reparación que ya hemos ido viendo en los capítulos anteriores. En primer lugar, consagra una “acción de reparación en naturaleza” para todas las infracciones cometidas por personas privadas u organismos públicos responsables del tratamiento de datos personales.

¹⁵⁵ “Reglamento del Registro de Bancos de Datos Personales a cargo de Organismos Públicos” contenido en el Decreto N° 799 del Ministerio de Justicia, que fue publicado en el Diario Oficial el día 11 de noviembre de 2000.

¹⁵⁶ Anguita y el profesor Daniel Álvarez entre otros, señalan que una de las mayores debilidades que posee la Ley N° 19.628 es la falta de un ente administrativo encargado de su cumplimiento, fiscalización y potestades sancionatorias, como expondremos en la unidad críticas doctrinarias a esta ley.

Esta primera acción es conocida como Habeas Data¹⁵⁷, que faculta al titular afectado para solicitar la eliminación, modificación o bloqueo de sus datos, y que tiene establecido un procedimiento especial de tramitación en los artículos 16 y 19.

En segundo lugar se establece la acción de indemnización de perjuicios por el daño patrimonial y moral que se siga del incumplimiento de algún deber de cuidado en el tratamiento de datos, como ya hemos explicado.

4.7.11 Habeas Data en la Ley N° 19.628

El artículo 16 de la Ley N° 19.628 consagra el llamado *Habeas Data*. Este *Habeas* es una acción judicial, específica y autónoma por medio del cual el titular de los datos personales a través de un conjunto de derechos (acceso, modificación, cancelación o bloqueo) puede proteger su privacidad, sus datos personales, frente a las acciones que resulten ilegales o arbitrarias o que importen un uso indebido de información de carácter personal que le concierne por parte del responsable del fichero o banco de datos.

¹⁵⁷ La acción de Habeas Data ha sido una de las innovaciones a la protección en este tipo de materias. Es ampliamente reconocido como una nueva garantía en Tratados Internacionales y en las Constituciones de Argentina, Brasil, España, Paraguay, Portugal, entre otros.

Esta expresión es escasamente utilizada por nuestra dogmática, en parte por una razón de texto. Aunque el artículo 16 de la Ley N° 19.628 utiliza la expresión “*amparo*”, en el artículo siguiente, sin embargo, se emplea el término “*reclamación*”.

A pesar de que el Habeas Data goza de consagración legal a través de la ley en comento, en la práctica las personas prefieren recurrir de protección en lugar de deducir esta acción, invocando una afectación a su honra, reputación o prestigio comercial, en vez de una a su vida privada. La razón de estos es muy simple y ocurre muy frecuentemente en el campo judicial incluso en otras áreas del derecho. La acción de protección es muy efectiva a la hora de restablecer los derechos de los afectados, sus costos de tramitación son menores, la jerarquía del tribunal competente, la rapidez que supone su procedimiento, y el eventual amparo a las personas jurídicas que no se encuentra en la Ley N° 19.628, en su caso, son algunas de las circunstancias que inciden en la opción por la vía constitucional a aquella especial prevista en la ley de protección de datos¹⁵⁸.

4.7.11.1 Causales de procedencia¹⁵⁹

Se desprenden del artículo 16 de la ley. La acción de Habeas Data se podrá deducir siempre que concurran los siguientes supuestos:

¹⁵⁸ PARADA, BÁRBARA. 2008. El régimen de responsabilidad civil en la protección de datos personales en Chile. Memoria de prueba para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile, Facultad de Derecho. p.65-66

¹⁵⁹ PARADA, BÁRBARA. "El régimen de responsabilidad civil en la protección de datos personales en Chile". op. cit., p.67

1. Cuando el responsable del registro o banco de datos personales “*no se pronunciare*” sobre una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales dentro de dos días hábiles¹⁶⁰.
2. Cuando el responsable del registro o base de datos “denegare” una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales por una “*causa distinta*” de la seguridad de la Nación o el interés nacional¹⁶¹.
3. Cuando el responsable del registro o banco de datos “denegare” una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales “*por motivos de seguridad de la nación o el interesa nacional*”¹⁶²
4. Con la modificación introducida por la ley N° 19.812¹⁶³ también se puede reclamar a través de este procedimiento, la infracción a los artículos 17 y 18 de la Ley N° 19.628.
5. Finalmente, por las infracciones que no estuvieren contempladas en los artículos 16 y 19 de la Ley N° 19.628¹⁶⁴

¹⁶⁰ Ley N° 19.628 artículo 16, inciso primero.

¹⁶¹ Ley N° 19.628 artículo 16, inciso primero.

¹⁶² Ley N° 19.628 artículo 16, inciso tercero.

¹⁶³ Publicada el 13 de junio de 2002.

¹⁶⁴ Ley N° 19.628 artículo 23, inciso segundo.

4.7.11.2 Legitimación activa y pasiva

La legitimación activa corresponderá al titular de los datos, que como ya sabemos, tiene que ser una persona natural.

La legitimación pasiva de la acción de *Habeas Data* recae en “el responsable del registro o banco de datos” que, como ya hemos visto, puede ser un particular o un organismo público. Si la acción se ejerce contra una persona jurídica, la acción se deducirá en contra de su o sus representantes legales.

4.7.11.3 Tribunal competente para conocer del Habeas Data

La Ley N° 19.628 dispuso dos procedimientos de reclamación. El titular de los datos personales deberá optar por el procedimiento según la causal invocada por el responsable de la base de datos para denegar la solicitud, así habrán dos tribunales competentes en primera instancia:

- a. Cuando el responsable del registro o base de datos “denegare” una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales por una “*causa distinta*” de la seguridad de la Nación o el interés

nacional, el titular de los datos tendrá derecho a recurrir al **juez de letras en lo civil** del domicilio del responsable, que se encuentre de turno según las reglas correspondientes¹⁶⁵.

- b. En caso de que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la nación o el interés nacional, la reclamación deberá deducirse ante la **Corte Suprema**, la que solicitara informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia¹⁶⁶.

4.7.11.4 Tramitación¹⁶⁷

Como señalamos en el punto anterior, la Ley N° 19.628 dispuso dos procedimientos de reclamación. El titular de los datos personales deberá optar por el procedimiento según la causal invocada por el responsable de la base de datos para denegar la solicitud:

¹⁶⁵ Ley N° 19.628 artículo 16, inciso primero.

¹⁶⁶ Ley N° 19.628 artículo 16, inciso tercero.

¹⁶⁷ ANGUIA RAMÍREZ, PEDRO. “La protección de datos personales y el derecho a la vida privada: Régimen jurídico, jurisprudencia y derecho comparado”. op. cit., p.316-319

4.7.11.4.1 Procedimiento Ordinario

.- Causales para denegar una solicitud:

- Impedir o entorpecer el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido.
- Afectar la reserva o secreto establecido en disposiciones legales o reglamentarias.
- Tratarse de datos personales almacenados por mandato legal, de los cuales no puede solicitarse la modificación, cancelación o bloqueo, fuera de los casos que contempla la respectiva ley.

.- Tribunal competente:

Como ya hemos visto, en este procedimiento el tribunal competente será en primera instancia, el juzgado de letras en lo civil que corresponde al domicilio del responsable de la base de datos que se encuentre de turno según las reglas generales. Y en segunda instancia, la Corte de Apelaciones, que conoce en sala.

.- Reglas por las cuales se rige el procedimiento judicial:

- Señalar claramente la infracción cometida y los hechos que la configuran
- Acompañar los medios de prueba que puedan acreditarlos, en su caso.
- Deducida la reclamación, el tribunal dispondrá su notificación por cédula, la cual debe dejarse en el domicilio del responsable del banco de datos correspondiente.
- Notificado el reclamo, el responsable del banco de datos debe presentar sus descargos dentro del 5° día hábil adjuntando los medios de prueba de los hechos en que los funda. En caso de que no disponga de ellos, debe expresar dicha circunstancia, caso en el cual el tribunal debe fijar una audiencia dentro de 5° día hábil para recibir la prueba ofrecida y no acompañada.
- El juez está facultado para adoptar todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que reconoce la Ley N° 19.628.
- El juez apreciara la prueba en conciencia.

- Se notificara por cedula la sentencia definitiva, la que se dictara en un plazo no mayor a 3 días de vencido el plazo establecido en el punto anterior con prescindencia de que se haya o no presentado descargos por parte del responsable del registro de datos. Si el tribunal decreto una audiencia de prueba, el plazo de tres días comienza una vez vencido el plazo fijado para esta audiencia.
- Todas las resoluciones del procedimiento, con excepción de la sentencia definitiva, se dictaran en única instancia y se notificaran por el estado diario.
- La sentencia definitiva será apelable en ambos efectos.
- Una vez deducida la apelación, el tribunal deberá elevar inmediatamente los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el Presidente de dicho tribunal deberá ordenar dar cuenta preferente del recurso sin esperar la comparecencia de las partes.
- La causa se conoce en cuenta. No obstante si la Corte de Apelaciones lo estima pertinente o se le solicita con fundamento plausible, podrá ordenar autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregará extraordinariamente a la tabla respectiva de la misma sala.

- La sentencia que se pronuncie sobre el recurso de apelación no será susceptible de ser impugnada por el recurso de casación.
- En caso de acogerse la reclamación, el tribunal deberá fijar en la misma sentencia un plazo prudencia para que se dé cumplimiento a lo resuelto y podrá aplicar una multa de 1 a 10 UTM. Si se trata de infracciones a lo dispuesto en los artículos 17 y 18 de la Ley N° 19.628, la multa que podrá imponer el juez va desde diez a cincuenta UTM¹⁶⁸.
- La falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decreta el tribunal, serán castigados con multas de dos a cincuenta unidades tributarias mensuales¹⁶⁹. En caso que el responsable del banco de datos fuese un organismo público, el tribunal podrá sancionar al jefe del servicio con la suspensión de su cargo por un lapso de cinco a quince días.

4.7.11.4.2 Procedimiento Especial

.- Requisitos de la acción de reclamación. El titular de los datos personales debe:

¹⁶⁸ La Ley N° 19.812, publicada en el Diario Oficial el 13 de junio de 2002, que modificó la Ley N° 19.628, dispuso multas más altas respecto a la infracción a los artículos citados incluidos en el Título III. En este caso el artículo 16, inciso quinto dispone las multas en comento.

¹⁶⁹ Ley N° 19.628 artículo 16, inciso sexto.

- Señalar claramente la infracción cometida y los hechos que la configuran.
- Acompañar los medios de prueba que los acrediten, en su caso.
- Deducida la reclamación, el tribunal dispondrá su notificación por cedula, la cual debe dejarse en el domicilio del responsable del banco de datos correspondiente.

.- Causales:

- Seguridad de la nación.
- Interés nacional.

.- Tribunal Competente:

- En única instancia la Corte Suprema que conoce en sala.

.-Disposiciones por las cuales se rige el procedimiento judicial:

- Denegada la solicitud del requirente por las causales expuestas, la reclamación deberá interponerse ante la Corte Suprema. El tribunal solicitara informe a la autoridad respectiva por la vía que considere más rápida y expedita, fijándole un plazo

- La causa se conoce en cuenta. No obstante, si la Corte lo estimare conveniente o se le solicita con fundamento plausible, podrá ordenar traer los autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregara extraordinariamente a la tabla respectiva de la misma sala.
- En caso de rendirse prueba, ésta deberá consignarse en cuaderno separado y reservado que conservará dicho carácter incluso después de afinada la causa su por sentencia ejecutoriada se denegare la solicitud del requirente.
- El tribunal apreciará la prueba en conciencia.
- El presidente del tribunal dispondrá que la audiencia no sea pública.
- En caso de acogerse la reclamación, el tribunal deberá fijar en la misma sentencia un plazo prudencia para que se dé cumplimiento a lo resuelto pudiendo aplicar una multa de una a diez UTM.
- La falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decrete el tribunal, serán castigados con multas de dos a cincuenta unidades tributarias mensuales.
- En caso de que el responsable del banco de datos fuese un organismo público, la corte podrá sancionar al jefe de servicio con la suspensión de su cargo por un lapso de cinco a quince días.

- En caso de que el tribunal acoja la reclamación, debe fijar en la misma sentencia un plazo que considere prudencial para dar cumplimiento a lo resuelto. Podrá aplicar una multa de una a diez UTM.
- Si el responsable de la base de datos personales no entrega en forma oportuna la información o retarda la modificación decretada por el tribunal, será castigado con multa de dos a cincuenta UTM.

4.7.12 Principales críticas a la ley N° 19.628

En este apartado, pretendemos revisar algunas de las visiones críticas sostenidas por algunos autores respecto a la ley N° 19.628. Debemos señalar primeramente que son muy pocos los autores que han estudiado a cabalidad el proceso de tramitación que condujo a la dictación de la ley N° 19.628 y a temas vinculados a ella. El intento por poder desarrollar una crítica a nuestro entender, carecería de innovación doctrinaria, pues, aunque son pocos los doctos que lo han hecho, han formulado sendas críticas que son sostenidas por todos los que se han involucrado en esta materia. De esta manera, nos limitaremos a exponer algunas de las principales críticas, y las cuales ha recogido el Profesor Pedro Anguita Ramírez en su libro sobre *“La Protección de Datos Personales y el Derecho a la Vida Privada”*.

Renato Jijena Leiva¹⁷⁰

El profesor Renato Jijena Leiva, ha venido desde la década de los ochenta desarrollando los temas relacionados con las materias que conforman los denominados sistemas de protección de datos personales. El profesor Jijena Leiva participo entregando sus observaciones tanto a la Cámara de Diputados como al Senado de la república durante la tramitación de la ley N° 19.628 aunque sus sugerencias y comentarios no fueron recogidos por el Congreso Nacional. Leiva critico fuertemente la ley señalando “...*que la protección legal de datos personales constituye un tópico jurídico con bastante perspectiva en países extranjeros, pero que en nuestro país constituye una realidad desconocida y poco estudiada*”¹⁷¹.

Sus principales cuestionamientos a la ley fueron:

- (Como ya hemos visto y apreciado) La inexistencia de un registro de responsables privados de bases de datos y de un órgano fiscalizador idóneo;
- Haber establecido como regla general que la información fuese pública y que no requiriese de la autorización de sus titulares para procesarse;

¹⁷⁰ Licenciado en Ciencias Jurídicas por la Pontificia Universidad Católica de Valparaíso, Diplomado en Derecho Informático por la Universidad de Zaragoza – España y Magister en Gobierno Electrónico - UTEM, Chile. JIJENA. [en línea] <<http://www.jijena.com/>> [acceso: 22 enero 2015].

¹⁷¹ ANGUITA RAMÍREZ, PEDRO. “La protección de datos personales y el derecho a la vida privada: Régimen jurídico, jurisprudencia y derecho comparado”. op. cit., p.332

- El no haber prohibido la transferencia internacional de datos personales a terceros países que no dispusiesen de un adecuado sistema de protección de datos¹⁷² y;
- El no haber exigido autorización previa para un cumulo enorme de actividades relacionadas con los datos personales como el marketing directo.

Jijena en un dejo de molestia afirmo:

“La ley chilena sobre protección de datos personales fue redactada a instancias de la asesoría de los grupos y empresas interesadas¹⁷³ en asegurar el lucrativo negocio que constituye el procesamiento de datos personales, lo que se sumó al desconocimiento inexcusable de los parlamentarios, que siguen jactándose de su autoría con fines de marketing”¹⁷⁴

¹⁷² Actualmente como dice Anguita: *“La Ley N° 19.628 no prohibió la transmisión de datos personales de los habitantes del país fuera del territorio nacional. Solo se refirió al envío de datos fuera de Chile en el artículo 5°, que aborda la transmisión automatizada de datos personales, operación que sujeta al cumplimiento de algunos requisitos. En dicho contexto declara inaplicables tales condiciones en los casos de transmisión de datos personales a organizaciones internacionales en cumplimiento de tratados o convenios”*. *Ibíd.*, p.332

¹⁷³ Las empresas a que hace mención Jijena son DICOM S.A., filial de la transnacional estadounidense Equifax, Asociación de Marketing Directo, Cámara de Comercio de Santiago y Cámara Nacional de Comercio de Chile. Renato Jijena Leiva, *“Comercio Electrónico, Firma Digital y Derecho. Análisis de la Ley N° 19.799”*, Editorial Jurídica de Chile, Santiago, Chile. En ANGUIA RAMÍREZ, PEDRO. *“La protección de datos personales y el derecho a la vida privada: Régimen jurídico, jurisprudencia y derecho comparado”*. *op. cit.*, p.332

¹⁷⁴ Jijena Leiva. *Ibíd.*, p.332

Claudio Magliona Markovitch¹⁷⁵

Dice Magliona que la creación de la ley N° 19.628 representa un progreso para el derecho informático nacional y para la protección de los derechos de las personas frente al tratamiento abusivo de sus datos personales, aunque sugirió introducir cambios a la ley, algunos de los cuales ya habían sido propuestos por Jijena.

Según Magliona, la ley N° 19.628 requiere incorporar las siguientes materias:

- La creación de un registro público de bases de datos privadas.
- La creación de un organismo administrativo regulador del funcionamiento de las bases de datos.
- La obligación de informar previamente por parte del responsable de una base de datos al titular de los datos respecto de los cuales se pretende efectuar un tratamiento.
- Establecer normas más precisas sobre la cesión de datos personales

¹⁷⁵ Abogado de la Universidad de Chile. *LLM in Law, Science & Technology* por la Universidad de *Stanford*. Director y Profesor del Magíster en Derecho y Nuevas Tecnologías de la Facultad de Derecho de la Universidad de Chile. CEDI 2015. Académicos. [en línea] <<http://www.derecho.uchile.cl/centro-de-estudios-en-derecho-informatico/quienes-somos/88570/academicos>> [acceso: 22 enero 2015].

- Estudiar la posibilidad de hacer extensiva las normas de la ley N° 19.628 a las personas jurídicas.
- Ampliar los casos en que el titular pueda oponerse a un procesamiento de sus datos.
- La posibilidad de exigir a los responsables de una base de datos la aplicación de medidas de seguridad concretas para evitar las filtraciones.
- Estudiar las facultades del Servicio de Registro Civil e Identificación respecto al registro de las bases de datos de los organismos públicos.
- Limitar la capacidad del Estado y sus organismos de excepcionarse del cumplimiento de la ley a casos específicos y restringidos¹⁷⁶.

¹⁷⁶ Claudio Magliona Marovitch, en “Chile: Protección de Datos Personales. Políticas de Privacidad”, publicado en Alfa-Redi, Revista de Derecho Informático, N° 101, febrero 2002, en <http://www.alfa-redi.org/revista/data/45-3.asp>. En ANGUIA RAMÍREZ, PEDRO. “La protección de datos personales y el derecho a la vida privada: Régimen jurídico, jurisprudencia y derecho comparado”. op. cit., p.332

¹⁷⁶ Jijena Leiva. *Ibíd.*, p.333

CAPITULO V

ANDROID, LAS .APP Y WHATSAPP

5.1 Android, el Sistema Operativo que cambió la historia

iOS y Android son los dos sistemas operativos más utilizados en los teléfonos móviles de última tecnología. El año de lanzamiento de estos sistemas operativos no solo coincide en lo que podría parecer una práctica de competencia comercial sino también en el hecho de que a esas alturas los teléfonos móviles habían alcanzado tal desarrollo tecnológico, que su hardware equivalía al de un computador de gama baja.

El primer teléfono móvil con Androide fue lanzado al mercado el 2 de octubre del año 2008¹⁷⁷, el T-Mobile G1¹⁷⁸ fue creado por la firma taiwanesa HTC. Android ya había sido lanzado casi un año antes en noviembre del 2007, pero solo aplicado por primera vez a un teléfono móvil el día que HTC lanzo a la venta el T-Mobile G1. Una noticia en una página web especializada decía *“A falta de probar el teléfono, el verdadero atractivo de este terminal no se ve a simple vista. Va en el interior y se llama Android. Al contrario que el sistema operativo del iPhone, Android es un*

¹⁷⁷ DIARIO LA NACIÓN. Presentan El Primer Celular con Android, el software de Google. [en línea] <<http://www.lanacion.com.ar/1052747-presentan-el-primer-celular-con-android-el-software-de-google>> [consulta: 22 enero 2015].

¹⁷⁸ XATAKA MÓVIL. T-MOBILE G1. [en línea] <<http://www.xataka.com/moviles/tmobile-g1>> [consulta: 22 enero 2015].

sistema operativo abierto, que permite su modificación y personalización (...) Llega junto con una tienda para aplicaciones, desde donde nos podremos descargar aplicaciones que la comunidad saque para este teléfono con Android (...) Donde de verdad se comporta de forma genial el teléfono G1 es en el trabajo con Internet. El navegador es similar al Safari de Apple para el iPhone, pero el verdadero potencial lo obtenemos cuando usamos los servicios de la empresa del buscador: Gmail, Google Maps, Calendar, Youtube, etc”¹⁷⁹.

Android al ser un SO basado en Linux, permite que las personas libremente desarrollen programas para ser utilizados en los dispositivos con Android, las llamadas .app o aplicaciones. De esta manera en unos pocos años la cantidad de aplicaciones ascendía a millones, y las personas podían tener en sus celulares programas para jugar, aprender a cocinar o hasta para predecir temblores.

5.2 Las .app

.app es la extensión utilizada para pequeños programas informáticos que pueden descargarse e instalarse en teléfonos inteligentes o Smartphone, y que permite a los usuarios ejecutar ciertas tareas en su teléfono.

¹⁷⁹ XATAKA MÓVIL. T-MOBILE G1.

Estos programas son también llamados aplicaciones, y la mayoría de ellas se encuentra agrupada en tiendas virtuales de pago¹⁸⁰ o de manera gratuita, dependiendo generalmente del sistema operativo (iOS, Android, Windows Phone, BlackBerry OS, etcétera). Actualmente las principales tiendas virtuales son; Android Market (Android), Play Store (Android) y App Store (iPhone, iPod, iPad).

Las app por lo general vienen en formato listos para usar. Hay millones de aplicaciones, para los más variadas necesidades, hay aplicaciones que simulan un personal training, simuladores de sonidos de aves, instrumentos musicales, armas, predecir temblores, ver televisión y películas, escuchar música, leer revistas, noticias, comics, mangas, para ver el saldo de nuestra tarjeta Bip, para saber el tiempo, juegos, comunicarse con otras personas a través de mensajería de texto, voz o videoconferencia, etcétera.

Como señalamos, cualquier persona con los conocimientos informáticos necesarios puede crear una .app, las que pueden ir siendo actualizadas a través del tiempo.

Algunas .app necesitan una conexión a internet para poder funcionar (como la aplicaciones para saber el saldo de nuestra tarjeta Bip, que se conecta a los servidores de Metro para obtener esta información), aunque generalmente después de instalarlas no es necesario tener una conexión a la red.

¹⁸⁰ Los llamados iPhone con sistema operativo iOS no permiten la distribución gratuita de toda aplicación desarrollada por terceros como si lo hace Android al ser un sistema basado en Linux, un sistema operativo de núcleo libre sin fines de lucro. Aunque todo aquel que desarrolle un software tiene el derecho a cobrar por él si así lo desea.

5.3 Android, “aplicaciones” y privacidad

Uno de los temas delicados de Android es la privacidad. Al ser Android un sistema operativo libre¹⁸¹, su configuración depende básicamente de sus usuarios y ya hemos repetido muchas veces la complejidad de desarrollar un SO o un software en general, así que podemos imaginarnos lo difícil que puede parecer esto. Como no todos los usuarios de Android son expertos en informática ni mucho menos en los conceptos ligados a esta rama, la mayoría de los usuarios no entienden muy bien donde ir cuando necesita hacer algo en Android o que quiere decir cada cosa en él.

Cuando arrancas Android por primera vez en tu teléfono móvil, tienes ese pequeño asistente que te ayuda a configurar tu cuenta de Google. Esta configuración es obligatoria si quieres usar tu Smartphone en toda su dimensión o solo quieres usarlo para comunicarte con él, de otra forma hubieras adquirido un teléfono móvil más básico. En nuestro caso, adquirimos un Smartphone modelo Galaxy Y S5360 de la marca Samsung.

Cuando quisimos utilizar el gestor de descargas Android Market apareció una pantalla que nos decía (y esto también sucedía si querías ejecutar alguna otra aplicación): *“Debes agregar una cuenta al dispositivo para continuar. ¿Deseas*

¹⁸¹ Android es un sistema operativo libre en el sentido que su código de programación puede ser alterado por cualquier persona, ya que, no existe un derecho de autor en su creador u otra persona, quien decidió que cualquiera podría modificar el sistema operativo a su gusto, permitiendo la utilización de Android sin límites.

agregarla ahora? y te entregaba dos opciones “*Si*” y “*No*”. Si escogías *NO*, cerraba el gestor y no podías acceder simplemente a las aplicaciones de Google en Android ni al gestor de descargas Android Market, en definitiva tu teléfono móvil no te permitía usar todas las prestaciones de un Smartphone mientras no agregaras una cuenta. Al escoger *Si*, se habría otra pantalla que decía: “*Agregar una cuenta de Google. Agregar una cuenta. Puedes utilizar más de una cuenta de Google en tu teléfono (como tu cuenta laboral y de hogar). Agregar una cuenta de Google sólo lleva algunos pasos. Toca “Siguiente” para continuar o presiona el botón “Atrás” de tu teléfono para salir*”. Al seleccionar siguiente te pedía ingresar los datos de una cuenta Google (en general es cuenta de Gmail). Al hacer esto luego aparecía otra ventana que decía: “*Hacer una copia de seguridad y restaurar. Puedes usar tu Cuenta de Google para hacer copias de seguridad de tus aplicaciones, de tu configuración (como favoritos y contraseñas de WiFi) y de otra información. Si ya hiciste copias de seguridad con esta cuenta puedes restaurarla a este dispositivo ahora*”. En donde aparecía una casilla para seleccionar que contenía lo siguiente: “*Hacer copias de seguridad para este dispositivo con mi Cuenta de Google constantemente*”. Luego de hacer clic en siguiente aparecía una pantalla señalando: “*Tu cuenta de Google ahora está vinculada a este teléfono. En este momento, las aplicaciones de Google están sincronizando datos. Cuando desaparezca el ícono “sincronización” de la barra de estado en la parte superior de tu pantalla, la descarga habrá finalizado*”.

Al finalizar la instalación, lo que básicamente hacía vincular tu teléfono a una cuenta, era darle una identificación a tu celular, así todo lo que hicieras básicamente con él tendría un sujeto determinado por su cuenta de Google (recuerda que al crear

una cuenta en Google te identificabas con un nombre, una edad, un domicilio, etcétera). Al finalizar, que en nuestro caso queríamos acceder a Android Market, actualizaba automáticamente Android Market a Play Store y te pedía aceptar los términos de uso, si tu rechazabas los términos de uso no podías bajar aplicaciones por medio de Play Store, que es el gestor de descarga para Android por defecto, otra disyuntiva, pues ya que habías vinculado tu cuenta a tu celular no era suficiente, debías aceptar los términos de servicio de Play Store, sino, no tendrías acceso a otras aplicaciones.

Como podemos ver, en ningún momento de la configuración de cuenta, se nos entregó alguna alternativa de configuración real, ni respecto a nuestra privacidad y otros temas, solo se limitaba a pedirte el ingreso de una cuenta de Google y de ahí en más el celular tenía acceso a tu cuenta directamente desde tu celular, todo lo que hicieras a través de la red con tu celular sería registrado y por defecto llevado a cabo bajo el nombre de esta cuenta vinculada necesariamente al inicio. Es cierto que como un OS libre puedes configurarlo a tu medida, pero para un usuario promedio esto es un desafío, preguntas como ¿dónde ir?, ¿qué hacer? y ¿qué significa tal o cual cosa? Son las preguntas más básicas que podríamos hacernos para al menos tener una noción de cómo hacerlo.

Otro problema común en Android son las aplicaciones. Toda persona con los conocimientos técnicos necesarios puede crear una aplicación para un celular con Android, sin limitación mayor que su propio conocimiento y un computador. Una persona puede crear una aplicación para aprender a cocinar y una persona interesada en aprender a cocinar la descargara e instalara en su teléfono móvil. Pero ¿sabemos

bien que estamos instalando en nuestro celular?, algunos dirán “Sí” una aplicación para aprender a cocinar, y es lo que parece, pero al instalarla esta aplicación puede tener otros objetivos ocultos, como darle completo control de acceso a la red, acceso a la memoria del teléfono, acceso en definitiva a tus datos.

Fácilmente podemos ver esto al instalar una aplicación gratuita, algunas después de instalarlas, instalan con ella otras aplicaciones, algunas llenan tu teléfono de publicidad, etcétera. Lo normal es que toda aplicación gratuita te descargue publicidad, ya que ese es el verdadero negocio de la .app gratuitas, no que tu pagues por ella, sino de vender publicidad a los usuarios. Pero otras van más allá y recogen de manera oculta información de tu teléfono, tus datos de llamada, tus preferencias, las páginas web que accedes, los datos de tus cuentas, tus archivos, etcétera.

A veces las aplicaciones que bajas e instalas señalan al momento de instalarlas las características del programa, pero luego que mucha gente la ha descargado lanzan una actualización que por lo general es automática que cambia completamente las características del software sin que tú lo sepas, y esta es una práctica que muchas aplicaciones llevan a cabo, que a todas luces son aplicaciones malignas, pero que se esconden bajo una inofensiva apariencia.

Existen otros casos donde el límite de lo legal no se muestra con claridad. Es el caso de aplicaciones como WhatsApp Messenger, una aplicación utilizada por millones de personas en todo el mundo, que permite a través de una conexión a internet enviar mensajes de texto de manera ilimitada y aparentemente gratuita, pero ¿qué gana WhatsApp con todo esto? Es una pregunta legítima, tal vez, los creadores

de WhatsApp son verdaderos filántropos que no buscan nada más que el bien de la humanidad, pero tal vez si ganen con WhatsApp ¿pero qué? y ¿cómo?, y ¿en que podría afectar esto a nuestra privacidad? Son solo algunas de las preguntas que intentaremos responder en el capítulo a continuación. Solo un ejemplo, el robo de información personal a los smartphome fue uno de los mayores problemas de vulnerabilidad informática del 2012¹⁸²

5.4 WhatsApp Messenger

En el mundo de las aplicaciones en donde existe una gran cantidad y variedad de ellas, son aquellas enfocadas a la comunicación las más descargadas y utilizadas por los usuarios en todo el mundo, especialmente las de mensajerías o chat¹⁸³. *WhatsApp Messenger* es una de estas aplicaciones para teléfonos celulares, y seguramente uno de los grandes éxitos de esta recién estrenada era del teléfono inteligente.

Conocida comúnmente como WhatsApp, el nombre de esta aplicación nace de un juego de palabras provenientes del inglés “What’s up” que al español podría traducirse como “¿Qué pasa?”, nombre que adquiere mucho sentido al entender de qué se trata esta .app .

¹⁸² EMOL. 2012 Robo de información y ataques a smartphones marcaron los problemas informáticos del 2012. [en línea]<<http://www.emol.com/noticias/tecnologia/2012/12/28/576743/robo-de-informacion-y-ataques-a-smartphones-marcaron-los-problemas-informaticos-del-2012.html>> [consulta: 22 enero 2015]

¹⁸³ Chat o Charla en español, designa una comunicación realizada de manera instantánea mediante el uso de un software y a través de internet entre dos o más personas.

WhatsApp, es un servicio de mensajería y chat para smartphone que soporta varios SO como iOS, Blackberry, Android y Symbian. Consiste en una aplicación que instalada en un Smartphone permite a dos o más usuarios comunicarse en tiempo real vía mensajes de texto, voz, imágenes o videos a costo que es casi cero (ya que usa la conexión 3G o Wifi de móvil), en donde el primer año es gratuito, luego la suscripción anual cuesta \$0.99 USD¹⁸⁴, y en Chile \$555¹⁸⁵. De este modo WhatsApp si gana en la compra y suscripción de su aplicación, lo que no es menor en la gran cantidad de usuarios que WhatsApp tiene en todo el mundo.

WhatsApp fue fundada en 2009 por Jan Koum, el jefe de plataforma de operaciones Yahoo, y Brian Acton, el responsable de ingeniería también de Yahoo. A finales del año 2011, a solo dos años de su creación, WhatsApp ya contaba con más de 100 millones de usuarios en todo el mundo¹⁸⁶, lo que hace de esta aplicación una de las más famosas y descargadas del globo.

Pero WhatsApp no solo se ha hecho famosa por ser una de las más importantes aplicaciones de mensajería instantánea, y poner en jaque a las grandes operadoras de telefonía móvil que han visto disminuido el uso de su servicio de sms, que poco a poco va quedando en desuso por tecnologías como WhatsApp. Sino también, por ser

¹⁸⁴WHATSAPP. 2015. WhatsApp FAQ - ¿Es gratis enviar mensajes WhatsApp? [en línea] <<http://www.whatsapp.com/faq/es/general/20965922>> [consulta: 22 enero 2015].

¹⁸⁵ Sin embargo, la experiencia ha demostrado que en nuestro país las personas no pagan por utilizar la aplicación, el servicio se renueva automáticamente una vez transcurrido el primer año o el siguiente.

¹⁸⁶ A mediados del año 2014, WhatsApp alcanzo 500 millones de usuarios en todo el mundo. WAYERLESS. 2014. WhatsApp marca un nuevo récord a dos meses de su compra por Facebook. [en línea] <<https://www.wayerless.com/2014/04/whatsapp-ya-tiene-500-millones-de-usuarios-activos/>> [consulta: 22 enero 2015]

una aplicación que pone en riesgo nuestra seguridad en lo que a nuestra privacidad respecta.

5.4.1 ¿Cómo funciona WhatsApp Messenger?

Cuando utilizas WhatsApp por primera vez, lo primero que aparece es una pantalla solicitándote vincular la aplicación a el número de teléfono celular en el cual estas instalando WhatsApp. Una vez hecho esto, la aplicación comprobara la veracidad de esta información, lo cual tomara algunos segundos, incluso minutos. Comprobado el hecho de que el número y tu celular coinciden, se podrá comenzara utilizar WhatsApp.

“Necesitamos tu número de teléfono porque así WhatsApp se direcciona mensajes entre tú y tus contactos, de forma parecida como lo haría SMS”¹⁸⁷.

Cuando escribes un mensaje en WhatsApp a algunos o varios de tus contactos y le das enviar, primeramente el mensaje va desde nuestro móvil a uno de los servidores de WhatsApp Messenger, para posteriormente ser enviado desde el servidor, en donde ha sido guardado, al móvil de la persona o personas a las que lo has enviado. El proceso de envío es casi instantáneo que físicamente es imposible imaginar todo este proceso, pero entre el móvil que envía el mensaje y el móvil que

¹⁸⁷ WHATSAPP. 2015. WhatsApp FAQ - ¿Por qué me pide el número de teléfono y acceso a mi lista de contactos? [en línea] <WhatsApp.com <<http://www.whatsapp.com/faq/es/general/20971813>> [consulta: 22 enero 2015].

lo recibe están los servidores de WhastApp. Esto puedes saberlo con los ticks o checks que aparecen a un lado de los mensajes que envías. Los ticks son importantes porque indican el estado de envió y recibo de un mensaje; un tick significa que el mensaje ha sido entregado al servidor y; dos ticks significa que el mensaje ha sido entregado al dispositivo de tu contacto¹⁸⁸. En un chat de grupo funciona de la misma manera, con la diferencia de que para que haya un doble check azul, todos deben haber leído el mensaje enviado. WhatsApp señala en su página web que en el caso de solo ver un ckeck verde, señalando que el mensaje solo ha sido enviado al servidor es porque¹⁸⁹:

- El móvil de la persona a quien envías está apagado o tiene batería baja / agotada.
- Puede ser que no tenga una conexión a internet (si está en un ascensor, si está en roaming o si no le queda disponible en el móvil).
- Puede ser que haya visto la notificación en la pantalla del móvil, pero no ha abierto WhatsApp para recibir el mensaje (muy común en el caso de iPhone).

¹⁸⁸ A finales del año 2014, WhatsApp implemento la modalidad del doble check azul, que permite informar al emisor del mensaje, que este ha sido leído por el receptor del mismo. EMOL. 2014. WhatsApp habría habilitado “doble check” para mensajes leídos. [en línea] <<http://www.emol.com/noticias/tecnologia/2014/11/05/688549/whatsapp-habria-habilitado-un-doble-check-azul-para-avisar-cuando-un-mensaje-fue-leido.html> [consulta: 22 enero 2015]

¹⁸⁹WHATSAPP. 2015. ¿Qué significan los ticks al lado de mis mensajes? [en línea] <<https://www.whatsapp.com/faq/es/general/20951546>> [consulta: 22 enero 2015]

- Puede ser que la persona a quien envías ese dormida, sobre todo si vive en otra parte del mundo.
- Puede ser que te haya bloqueado.

5.4.2 Seguridad en WhatsApp Messenger

Para explicar cómo funciona la seguridad en WhatsApp, deberemos ocupar un lenguaje más técnico propio de la informática, aunque es importante entender la idea central, intentaremos explicar de la manera más simple los conceptos que puedan parecer ajenos a nuestro normal conocimiento del tema.

En un lenguaje más técnico WhatsApp Messenger ocupa como destino un puerto de comunicación HTTPS cuyo número es 443¹⁹⁰, donde el mensaje viaja en texto plano, es decir, solo caracteres sin ningún formato, lo que permite que el mensaje se pueda leer de manera simple sin tener que ser interpretado por algún experto de la programación, y no solo el mensaje, sino el nickname, número de teléfono, etcétera. La aplicación utiliza el protocolo XMPP (una tecnología abierta de comunicación en tiempo real muy potente y utilizado actualmente por los programas de chat o mensajería). Como mecanismo de autenticación WhatsApp ha

¹⁹⁰ Toda conexión que realizamos hacia un servidor a través de internet, se hace a través de un puerto con un número, así un juego usara un tipo determinado de puerto, algunas otras conexiones se harán por puertos aleatorios para garantizar la fluidez, etcétera. Es una vía de comunicación entre el servidor y el cliente.

optado por SASL DIGEST-MD5¹⁹¹, el cual utiliza los siguientes valores para generar el challenge (MD5): username, password, realm, nonce, cnonce, nc, digest-uri y qop. Todos estos datos menos el nombre de usuario y password (contraseña) son generados por el servidor o cliente y se envían en el challenge. El nombre de usuario lo proporciona el cliente y también es enviado, y por último el password también se utiliza para generar el MD5 pero no se envía, ya que es el valor que permite que la autenticación con el servidor sea segura¹⁹².

Cuando explicamos al principio de este punto como funciona WhatsApp, señalamos que durante la instalación, vinculábamos nuestro teléfono móvil con la aplicación ingresando nuestro número telefónico, pero nunca una contraseña. Al respecto los programadores se debaten en una discusión sobre este método de seguridad, ya que, no es normal que MD5 genere una contraseña, por lo que ha debido ser agregada por los creadores de whatsApp, es decir, no sería posible bajo este mecanismo de seguridad generar una contraseña diferente para cada mensaje porque MD5 no hace esto por sí mismo, entonces lo más probable es que sea una contraseña genérica (igual) para todos los mensajes. Lo anterior en simples palabras significaría que el que descubriera esta contraseña podría fácilmente burlar esta seguridad y solo con el número de teléfono y esta password genérica, tener acceso a todas nuestras conversaciones, incluso las borradas, ya que todas se guardan por algún tiempo en los servidores de WhatsApp.

¹⁹¹ IETF. 2000. Mecanismo que permite la comunicación segura entre servidor y cliente. Microsoft: 'Using Digest Authentication as a SASL Mechanism. [en línea] <<http://www.ietf.org/rfc/rfc2831.txt>> [consulta: 22 enero 2015].

¹⁹² SECURITY BY DEFAULT. 2011. WhatsApp y Su Seguridad, ¿pwn3d? [en línea] <<http://www.securitybydefault.com/2011/03/whatsapp-y-su-seguridad-pwn3d.html>> [consulta: 22 enero 2015]

Sin embargo, se señala que: “El auténtico problema de seguridad en Whatsapp no está en la falsa encriptación que utiliza. El gran fallo está en cómo te identificas en Whatsapp, y en lo fácil que es para alguien con interés conectarse en tu nombre: sólo hace falta que el interesado conozca tu número de teléfono, y tu IMEI en el caso de Android, o tu dirección MAC en el caso de iPhone”¹⁹³.

En otro punto de seguridad en WhatsApp, dentro de la memoria de nuestro celular están nuestros archivos. WhatsApp genera una carpeta con el mismo nombre de la aplicación para guardar y administrar los archivos necesarios para la gestión y funcionamiento de WhatsApp. Dentro hay una carpeta llamada Databases, en esta carpeta están todas las conversaciones o mensajes en .db¹⁹⁴ que hemos realizado por WhatsApp, incluso las borradas, de esta manera aunque borremos las conversaciones desde la aplicación, están seguirán estando tanto en los servidores de WhatsApp como en la memoria de nuestro celular.

Otro problema está en el hecho de si tu celular se extravía o si te lo han robado o hurtado, y aparte de que alguien pueda obtener tus conversaciones, pueda seguir usando tu WhatsApp. La empresa señala que deberemos notificar a WhatsApp inmediatamente de cualquier violación de seguridad o uso no autorizado de nuestro teléfono móvil, esto incluye claramente el caso de extravió, robo o hurto. Aunque

193 XATAKA MÓVIL. 2012 Seguridad usando Whatsapp: Lo estás haciendo mal. [en línea] <<http://www.xatakamovil.com/seguridad/seguridad-en-whatsapp-lo-estas-haciendo-mal>> [consulta: 22 enero 2015]

¹⁹⁴ Un archivo de base de datos que puede ser leído con programas como Microsoft Office Acces y Microsoft Office Excel entre otros.

señala que WhatsApp no será responsable de las pérdidas y la mala utilización causadas por el uso no autorizado de su cuenta¹⁹⁵.

5.4.3 Términos de Servicio

Los Términos de Servicio así como la Política de Privacidad de WhatsApp, son analizados a la versión del 07 de julio de 2012, que es la última modificación a la fecha de este trabajo.

Lo primero que podremos notar es que en su página web WhatsApp solo tiene una versión en idioma inglés de su Política de Privacidad y Términos de Servicio, lo que claramente dificulta el entendimiento de las personas que no manejan este idioma.

Los términos de servicio se dividen en once puntos¹⁹⁶. Los que a continuación analizaremos, sintetizando las ideas más importantes de cada uno de ellos:

¹⁹⁵ Al final de la letra B del punto 3 de los Términos de Servicio de WhatsApp, esta señala que: “*You must notify WhatsApp immediately of any breach of security or unauthorized use of your mobile phone. Although WhatsApp will not be liable for your losses caused by any unauthorized use of your account, you may be liable for the losses of WhatsApp or others due to such unauthorized use*”. WHATSAPP. 2012. Información legal de WhatsApp. [en línea] <<https://www.whatsapp.com/legal/>> [consulta: 22 enero 2015]

¹⁹⁶ Los once puntos son: 1) our Acceptance (Su aceptación); 2) WhatsApp Service (Servicio WhatsApp); 3) WhatsApp Acces (Acceso WhatsApp); 4) Intellectual Property Rights (Derechos de Propiedad Intelectual); 5) User Status Submissions (Envío de estado de usuario); 6) Warranty Disclaimer (Renuncia de garantía); 7) Limitation of Liability

1. Tu Aceptas

Este primer punto señala básicamente que el usuario entiende y acepta estas Condiciones de Uso, y la Política de Privacidad incluida por referencia. Si no estás de acuerdo con estos términos y condiciones no podrás utilizar el servicio.

2. Servicio WhatsApp

Estas Condiciones de Uso se aplican a todos los usuarios del Servicio WhatsApp. Y lo que es el servicio WhatsApp se indica en el punto 1: el software, el cliente y sitio web de WhatsApp, así como todo el contenido disponible a través del cliente y la web. Es decir, a no ser que se indique lo contrario, estas Condiciones de Uso se aplican a todo lo que lleve la palabra WhatsApp o se derive de ella.

Luego se indica lo que será la primera excepción de responsabilidad, por cuestión de enlaces en este caso. Dice WhatsApp que a través de las actualizaciones de estado o mensajes puede haber enlaces a páginas web de terceros que no son propiedad de o están controladas por WhatsApp. Por ese motivo, no asume responsabilidades respecto al contenido, políticas de privacidad o prácticas de esos sitios. Además, dice WhatsApp que no puede censurar o editar el contenido de una página web de un tercero.

(Limitación de responsabilidad); 8) Indemnity (Indemnidad entendido como libertad de perjuicio); 9) Ability to Accept Terms of Service (Capacidad para aceptar los Términos de Servicio); 10) Assignment (Asignación); 11) General.

Termina señalando que por el hecho de usar el servicio no se hará responsable a WhatsApp de los posibles daños, reclamos o responsabilidad que surja del uso por parte de WhatsApp de páginas web de terceros encontrados usando el servicio.

3. Acceso a WhatsApp

Este punto contiene tres literales.

En el literal A de este punto, se establece que si aceptamos estas Condiciones de Uso, WhatsApp aún no nos permite usar el servicio, antes tenemos que hacer algo más. Aceptar y cumplir los 4 puntos siguientes:

- 1) El uso del servicio es exclusivamente personal, no se puede revender o cobrar a otros por su uso o acceso ni actuar en cualquier otra forma inconsistente con estas condiciones.
- 2) No podemos duplicar, transferir, dar acceso a, copiar o distribuir ninguna parte de WhatsApp, con independencia del medio, si no tenemos la autorización por escrito de WhatsApp.
- 3) No se puede modificar WhatsApp, en todo o en parte. En este sentido, cualquier uso de una aplicación que nos permitiera modificar la estética de WhatsApp estaría violando este punto.

4) Finalmente, debemos cumplir con los términos y condiciones de estas *Condiciones de Uso*; que recuerdo, también incluyen por referencia la Política de Privacidad.

En el literal B, WhatsApp nos indica que para poder acceder y utilizar las funciones del Servicio, se debe reconocer y aceptar que tendremos que proporcionar a WhatsApp nuestro número de teléfono móvil. Además aceptamos que WhatsApp periódicamente puede acceder a nuestra lista de contactos y/o libreta de direcciones para buscar y realizar un seguimiento de los números de teléfono móvil que también usan el servicio. Al proporcionar nuestro número de teléfono móvil damos nuestro consentimiento expreso para que WhatsApp pueda acceder a la lista de contactos y/o libreta de direcciones con el fin de proporcionar y utilizar el Servicio. Señala WhatsApp que al recoger esta información no se recopilan nombres, direcciones o direcciones de correo electrónico, solo el número de teléfono móvil. El usuario será el único responsable de los mensajes de estado que envía y de que se muestre el número de su teléfono móvil en el servicio. Además, se señala que WhatsApp no puede usar el número de teléfono de otra persona sin su permiso, y he aquí la disyuntiva de que si ellos pueden acceder a todos mis números telefónicos, sí están usando el número de otras personas, la cuestión es que WhatsApp lo hace para verificar quien usa el servicio y quien no, y quien usa el servicio, sí ha dado de antemano su consentimiento.

Finalmente, si se pone en peligro la seguridad de nuestro teléfono o se hace un uso no autorizado del mismo, sea por hurto, robo o simple extravió, debemos

notificarlo inmediatamente a WhatsApp, que en ningún caso será responsable de los daños o pérdidas que podamos sufrir por un mal uso de nuestra cuenta.

En el literal C se utilizan muchos tecnicismos informáticos, haciendo referencia a programas capaz de recoger información desde un computador o en este caso un servidor, también de programas que puedan generar muchos mensajes en un periodo de tiempo en el que un humano no podría hacerlo saturando los servidores de WhatsApp (a eso hace referencia con los “load testers”). Luego señala que WhatsApp si permite a los buscadores (como Google) usar “spiders” o arañas (que básicamente son programas para copiar contenidos) para copiar materiales de la web de WhatsApp con la finalidad de que se creen índices que puedan ser encontrados por aquel que utiliza el buscador, y que WhatsApp tiene el derecho a revocar todo lo anterior.

Más adelante en este literal C. vuelve a reafirmar un poco lo que señala al principio, especificando que no están en contra en el uso de algunos programas como sniffer (lo que se traduciría como “olfateadores”) o analizadores de paquetes¹⁹⁷, pero sí de cualquier intento por hacer ingeniería inversa de su sistema de protocolos, o explorar el sitio más allá de los límites normales generados por el cliente de WhatsApp. Por esa razón no permiten herramientas que pretendan explorar, dañar o testear el sitio. Si eso se pretende, requieren el consentimiento o permiso expreso de WhatsApp.

¹⁹⁷ Programas que pueden recoger información en una red, por eso se les llama “olfateadores” porque buscan algo que les interese y lo recogen. En esta parte WhatsApp no hace alusión a la información de las personas o sus datos, sino información pública de WhatsApp, como su página web, etcétera.

Al final WhatsApp se compromete a no recolectar información personal identificable, como puedan ser nombres de usuario, o usar el servicio para spam¹⁹⁸ o comunicaciones comerciales. Por esa misma razón también se comprometen a no hacer solicitudes a los usuarios del servicio con finalidad comercial, sobre sus actualizaciones de estado o User Status Submissions¹⁹⁹.

4. Derechos de propiedad intelectual

Todo lo relacionado con WhatsApp, menos los mensajes o actualizaciones de estado del usuario, es propiedad de WhatsApp o esta licenciado a su favor. Así como vimos en el punto 3 (i), se vuelve a insistir en que el servicio es solo para uso personal. Lo que no queda claro es si una persona de manera no habitual puede enviar publicidad por WhatsApp, sí yo personalmente envié a mis contactos un mensaje que diga “Vendo cervezas si tienen sed”, ¿hasta qué punto no es un uso personal? ¿es tan claro que es un uso netamente comercial? Me parece que la idea de WhatsApp es evitar este tipo de prácticas, ya que, ha sido reiterativo al señalar su uso personal, pero al menos WhatsApp se reserva el derecho de hacerlo eventualmente. Habría que ver el fin con que se utiliza el servicio, pero queda claro entonces que si este fin es netamente comercial no se podría usar el servicio, debe ser personal, y enviarle a tus contactos una publicidad no sería usar el servicio de manera no personal, ya que personalmente, puedo señalarle a mis “amigos” que vendo tal cosa para que sepan, en ningún caso estoy haciendo un negocio a través de

¹⁹⁸ “Son mensajes no solicitados enviados en forma masiva, generalmente de tipo comercial o publicitario. Llegan por diferentes vías: correo electrónico, correo postal, celulares, fax, etc., siendo los más comunes aquellos enviados por internet”. BIBLIOTECA DEL CONGRESO NACIONAL. 2012 Spam. [en línea] <http://www.bcn.cl/leyfacil/recurso?item_id=4840&leng=es> [consulta: 09 septiembre 2014].

¹⁹⁹ Lo que no significa que otros si puedan hacerlo usando el servicio de WhatsApp. Esto lo veremos más adelante.

WhatsApp, lo ocupo con un fin personal no completamente comercial, como dice el refrán “una golondrina no hace verano”.

5. Presentaciones de estado de usuarios

Este punto contiene hasta un literal F.

Lo más importante del literal A, es el hecho de que cualquier persona que tenga tu número telefónico puede ver tu estado, tu ultima conexión (esta información la publica WhastApp al conectarte al servicio) y tu foto de perfil de WhatsApp. Más concretamente se señala que estos tres datos pueden ser vistos a nivel mundial y que uno entiende que si dichos archivos se publicaron, WhatsApp no garantiza ningún tipo de confidencialidad al respecto. En la actualidad, WhatsApp no tiene ningún método para proporcionar diferentes niveles de visibilidad de los envíos de estado entre los usuarios que tienen nuestro número telefónico.

Podemos ver que ya hay tres datos que al momento de publicarlas en WhatsApp podrán ser públicas mundialmente: Nuestro estado, nuestra última conexión a la publicación y nuestra foto de perfil. Esta es sola la punta del iceberg en cuanto a los riesgos que puede sufrir nuestra privacidad al respecto, la más visible y, tal vez, la menos dañina como ya podemos ir apreciando.

En el literal B es importante señalar que WhatsApp se define como “repositorio de datos”, es decir, un depósito de datos, y en ningún caso se hace responsable de las actualizaciones de estado y la foto de perfil enviada por los usuarios, ya que, no

representan las opiniones de WhatsApp y tampoco garantiza la validez, certeza o legalidad de las mismas. Pensemos por ejemplo una persona que tiene en su foto de perfil, la foto de una menor de edad desnudo, esto podría ser ilegal, en este caso WhatsApp no se hace responsable. La propiedad de las actualizaciones de estado son del usuario, pero para ello el usuario antes debe tener los derechos sobre esas actualizaciones de estado.

En la sección C se establece una serie de compromisos que debe cumplir el usuario en relación a los envíos de estado. Principalmente destacaremos el hecho de que los usuarios se comprometen a no presentar material que tiene derechos de autor, protegidos por el secreto comercial o sujetos a otro tipo de derechos de propiedad de terceros, incluidos los **derechos de privacidad** y publicidad, a menos que sea el dueño de dichos derechos o tenga permiso de su legítimo propietario para publicarlos, concediéndole a WhatsApp todos los derechos de licencia otorgados por este documento.

El literal D establece que el contenido para adultos de los estados debe ser identificado como tal, ¿cómo? ¿dónde? es una cuestión que no queda claro, deberá ser probablemente en el mismo mensaje de estado.

WhatsApp se reserva el derecho de eliminar el contenido y estado de envíos sin previo aviso. También podrá cancelar el acceso de un usuario al servicio, si determina que es infractor reincidente (entendido como alguien que ha sido notificado más de una vez por actividad infractora, o han sido sus actualizaciones de estado o mensajes eliminados de la página web con anterioridad) o nos ha cancelado

el servicio más de dos veces por cualquier o ninguna razón además de ser molesto. También se nos puede cancelar el servicio por ser molesto –como señalamos-, algo que determinará personal autorizado de WhatsApp o un *superheros* (superhéroe, que imaginamos es lógicamente una broma) o se pueden eliminar actualizaciones de estado o mensajes nuestros por ser demasiado largos o tener poco interés.

En E se señala que a través de las actualizaciones de estado que nos lleguen vía WhatsApp, podemos encontrarnos expuestos a una variedad de fuentes y archivos de estado que pueden ser inexactos, ofensivos, indecentes o censurables. Que al aceptar estas condiciones renunciamos a cualquier derecho legal o recurso que tengamos o pudiéramos tener contra WhatsApp al respecto, en la máxima medida permitida por la ley.

Por último la sección F, nos señala que tenemos permiso de WhatsApp para vincular contenidos del servicio, pero sólo para uso personal -cuestión que se reitera una vez más, el carácter personal del uso del servicio-.

6. Exención de la Garantía

Podemos resumir este punto, como el hecho de que la persona acepta el uso del servicio bajo su propio riesgo. En la **medida máxima permitida por la ley**, WhastApp y sus funcionarios no se hacen responsables de nada, en ningún caso.

7. Limitación de Responsabilidad

Este punto es una extensión del punto anterior. En ella WhatsApp refuerza la idea de que no se hace responsable de los daños, pérdidas o perjuicios por el uso de la aplicación. Del punto (III) podemos inferir la importancia de no enviar datos sensibles, ya que, WhatsApp no se hará responsable por ellos.

WhatsApp servicio es controlado y ofrecido desde sus instalaciones en los Estados Unidos de América, y alguien que accede o utiliza WhatsApp desde otros países o desde otras jurisdicciones lo hace por su propia voluntad y responsabilidad.

8. Indemnidad

Este punto que se titula indemnidad, básicamente señala que si hacemos algo mal o infringimos estas condiciones de uso en algún sentido, WhatsApp no es responsable, sino nosotros, e inclusive deberemos indemnizar a WhatsApp o a terceras personas si se ven afectadas por nuestro actuar.

Al final agrega algo que también nos parece una broma por parte de la empresa y que no viene al caso, es la última frase que traducida dice más o menos así; *“No apoyamos ni alentamos el consumo ilegal de alcohol o tabaco, para que lo sepas”*.

9. Capacidad de aceptar los términos de servicio

Para poder aceptar los Términos de Servicio debo ser mayor a 16 años, ser menor emancipado o disponer del consentimiento de los padres o del tutor. Ser plenamente

capaz y competente para entender los términos, condiciones, obligaciones, afirmaciones, declaraciones y garantías establecidas en estos Términos de Servicio, y de poder cumplirlas. Quien tiene menos de 16 años no está autorizado a usar WhatsApp.

Además, no debo vivir en un país sujeto a embargo por el Gobierno de los Estados Unidos, o que haya sido designado terrorista o de ayudar al terrorismo (que sería a los ojos de EE.UU. lo mismo) y que no están restringidos de alguna forma por el Gobierno de EE.UU.

10.Destino

No podemos ceder o transferir estas Condiciones de Uso ni los derechos y licencias garantizadas por las mismas, WhatsApp sí puede hacerlo sin restricción alguna.

11.General

Finalmente, WhatsApp señala que la jurisdicción de cualquier reclamación o disputa entre el usuario y WhatsApp será resuelta exclusivamente por el tribunal de jurisdicción competente del condado de Santa Clara, California (lo que en la mayoría de los casos se traduciría en indefensión).

Estos Términos de Servicio, Política de Privacidad y cualquier otro aviso legal, son los términos y condiciones que el usuario y WhatsApp “firmamos” en relación a la app y su servicio.

La nulidad que pudiera afectar a una condición no invalida la totalidad de las condiciones.

WhatsApp se reserva el derecho a enmendar o modificar estos Términos de Servicio en cualquier momento, y es responsabilidad del usuario revisar estos términos y cualquier cambio. El uso continuado del servicio tras una modificación de estas condiciones, significara su consentimiento y aceptación tácita de los nuevos términos.

5.4.4 Política de Privacidad²⁰⁰

En cuanto a la Política de Privacidad que se titula ***Privacy Notice*** (“Aviso de Privacidad” o “Confidencialidad”), destacaremos los puntos más importantes a nuestro entender:

“Por favor, tenga en cuenta que cualquier Presentación de estado o de otros contenidos publicados en la dirección o la discreción de los usuarios del Servicio WhatsApp se convierte en contenido publicado y no se considerara información de identificación personal sujeto a esta Política de Privacidad”.

²⁰⁰ WHATSAPP.2015. WhatsApp: Legal. [en línea] <<http://www.whatsapp.com/legal/#Privacy>> [consulta: 22 enero 2015].

Como ya lo explicamos en el punto 5 de los Términos de Servicio (*User Status Submissions*), el mensaje de estado, tu última conexión y tu foto de perfil no serán información personal sujeta a esta Política de Privacidad, ya que, es una información pública a nivel mundial, y uno entiende como tal, que lo son al aceptar los términos de servicio.

“WhatsApp puede obtener los siguientes tipos de información de o acerca de ti o tu dispositivo móvil, que puede incluir información que puede ser utilizada para identificarle a usted como se especifica más adelante (“Información de Identificación Personal”):

Información Provista por el Usuario (...)

Cookies de Información (...)

Archivo de log (...)

Respecto a la información provista por el usuario, WhatsApp puede obtener información sobre:

- Tú número de teléfono celular

- Tu nombre de estado (si procede)

- Información de facturación (si es aplicable, es decir, si pagas por el servicio)

- Información del dispositivo (modelo y marca de teléfono móvil)
- Tu libreta de direcciones o lista de contactos, a la cual WhatsApp podrá acceder periódicamente para localizar quienes usan WhatsApp y quiénes no.

Respecto a las Cookies²⁰¹, WhatsApp envía dos clases de cookies a nuestro ordenador cuando visitamos su página web, una cookie persistente y una cookie de sesión. La cookie persistente se aloja en nuestro computador y la cookie de sesión solo es temporal y desaparece cuando dejamos de visitar la página web de WhatsApp. Los navegadores web permiten que se puedan rechazar todas las cookies que puedan ser enviadas a nuestro computador, pero esto puede hacer que algunas páginas no funcionen de la manera más correcta, de todas maneras queda a criterio del usuario.

Los archivos de log (archivos que nos identifican), son datos que los servidores de WhatsApp registran cada vez que utilizamos su sitio web. Entre estas informaciones están nuestra IP (que sería el nombre de nuestro computador en la red), tipo de navegador que usamos al momento de visitar la página web, numero de clic que damos y donde los damos en la página (así ellos saben que es lo que más se visita de su web), la cantidad de tiempo invertido en cada página o sesión, la fecha y hora de conexión, nuestro número de teléfono si navegamos en él, etcétera.

Respecto a la información que el servicio no recoge, WhatsApp señala:

²⁰¹ Las cookies son pequeños archivos de texto que permiten recoger información del usuario, como sus preferencias, páginas web que visita, que le gusta, sus cuentas y contraseñas, etcétera. Todo para hacer más rápida y expedita la navegación por internet.

WhatsApp no recoge la siguiente información: a) los nombres; b) correos electrónicos; c) direcciones u otra información de contacto de la libreta de direcciones de los usuarios móviles o listas de contacto. Lo único que recoge WhatsApp es el número de teléfono móvil y el nombre que le hayamos asignado a ese número de teléfono móvil, ejemplo de ellos sería: *Hermano 77665532*.

La compañía también explica que es lo que hace con los mensajes, imágenes, sonidos y videos que las personas envían en sus conversaciones. Básicamente explican que los mensajes que han sido enviados y pasan por los servidores de WhatsApp no se copian (esto toma razón cuando expliquemos más abajo que pasa con estos mensajes). Los mensajes que son enviados a los servidores pero que no han podido ser enviados al destinatario por algún motivo de los que hemos explicado en el punto 8.4.1, si no se pueden entregar en un lapso no mayor a 30 días, serán eliminados después de cumplido este plazo. **Los mensajes que se envié por el servicio y hayan sido entregados a sus destinatarios, no se guardan ni son retenidos por los servidores, se borran**, el único registro que queda en los servidores son el remitente y el destinatario del dispositivo móvil (y que pueden ser eliminados a discreción del usuario). No obstante lo anterior, WhatsApp si puede retener información de la fecha y el tiempo en que han sido enviado los mensajes que han sido entregados con éxito y los números de teléfonos móviles que intervienen en los mensajes, así como cualquier otra información que WhatsApp este legalmente obligado a recoger.

Respecto a los archivos que se envié (como imágenes, sonidos y videos), residirán en los servidores de WhatsApp después de entregados por un corto periodo

de tiempo (¿Qué quiere decir con un corto periodo de tiempo?) de acuerdo con sus políticas de retención general (¿dónde están? al menos en su página web no están).

Respecto de cómo WhatsApp utiliza la información señala: El número de nuestro teléfono móvil se conservara. Nuestra información de facturación se eliminara solo al cabo de 30 días siguientes a la terminación del servicio.

Más adelante WhatsApp vuelve a señalar qué información es pública (estado, foto de perfil y “ultima vez”).

WhatsApp puede recoger nuestro número (que no es nada nuevo) y nuestro mail (lo obtendrán básicamente de si esta en nuestro teléfono móvil o si nos contactamos con WhatsApp) para comunicarnos con el objetivo de servicio al cliente, en ningún caso para información comercial, aunque información de servicio al cliente es amplio, si existe una mejora en WhatsApp que es pagada y nos comunican para adquirirla ¿será una información comercial o de servicio al cliente? Señala que puede adquirir información cuando navegamos por su página web, lo que explicamos que hace a través de las *cookies* o *archivos log*, y utilizarlas para mejorar el servicio de página web.

Otro punto trata de la información que WhatsApp revela Allí vuelve a repetir que tu estado, foto y la notificación de “ultima vez” (ultima conexión a la aplicación que sale en el estado y que agrega WhatsApp) es pública para cualquiera que tenga el número de tu teléfono celular.

WhatsApp no vende ni comparte información de identificación personal - dando el ejemplo del número de teléfono móvil, que sería el dato más ínfimo de nuestra información personal- con otras empresas de terceros para su uso comercial o de marketing a menos que demos nuestro consentimiento para ello - consentimiento que ya hemos dado al aceptar los Términos de Servicio-.

WhatsApp puede compartir información con terceros proveedores de servicios para mejorar o mantener el propio servicio de WhatsApp.

WhatsApp puede recopilar información y divulgar aquella que es personal identificable o no, si así lo requiere la ley o creen de buena fe que dicha acción es necesaria para cumplir las leyes estatales (como en EE.UU. Ley de Propiedad Intelectual), el derecho internacional, responder a una orden judicial, citación u orden de allanamiento o equivalente, o cuando razonablemente creen que está en peligro o amenazada la seguridad física de un individuo²⁰².

Además, WhatsApp también se reserva el derecho a revelar información de identificación personal o no, cuando se cree de buena fe, que es apropiado o necesario para hacer cumplir los Términos de Servicio, tomar precauciones de responsabilidad, para investigar y defenderse contra cualquier reclamación de terceros o alegaciones, para ayudar a los organismos gubernamentales encargados de hacer cumplir la ley²⁰³, para proteger la seguridad e integridad del Sitio Web o de los servidores de la

²⁰² Por ejemplo se estructura un crimen por WhatsApp.

²⁰³ Por ejemplo, podría solicitarse a WhatsApp a través de una orden judicial la revelación de información personal de acusado por terrorismo. En este caso WhatsApp deberá entregar la información que posea en su poder, como números de teléfono, archivos, conversaciones (si no las ha borrado según su política de privacidad), fecha y hora de estos mensajes o conversaciones, etcétera.

empresa, y para proteger los derechos de propiedad o seguridad personal de WhatsApp, de los usuarios y terceros.

Uno como usuario tiene la opción de eliminar la cuenta si no está conforme con los Términos de Uso y Política de Privacidad.

La empresa señala que para proteger nuestra privacidad y seguridad, se tomaran todas las medidas razonables (tales como la autenticación de mensajes en ciertos casos) para verificar su identidad antes de registrar el número de teléfono móvil y permitirnos acceso al servicio.

Si tenemos quejas, dudas o sugerencias podemos contactarnos a través de su página web, enlace *Contacto*.

En su tono tan singular como ya hemos visto, WhatsApp dice “*No somos fanáticos de la Publicidad*”. WhatsApp es libre de publicidad hasta que no cambien de opinión y modifiquen este punto, para lo cual deberemos estar atentos. Es nuestra responsabilidad revisar cualquier modificación a los Términos de Servicio y Políticas de Privacidad.

Respecto a la seguridad de los datos, WhatsApp se compromete a tomar todas las providencias necesarias para garantizar la seguridad de la información, pero no puede garantizar la seguridad de la información, – la idea es que lo intentan aunque no aseguran que lo hagan – todo es bajo nuestro propio riesgo. WhatsApp dice que ellos mismos pueden bajo su propia iniciativa revelar la información, en los casos

que ya vimos. Cualquier fallo de seguridad electrónica que afecte a WhatsApp se informara en su sitio web.

La empresa garantiza que no recopila y mantiene información de niños menores de 16 años de edad. Si una persona transmite información identificable de un menor de edad – que pueda ir en el estado o foto de perfil – se podrá desactivar la cuenta y bloquear el estado. Al final dice *“Y Siempre pensar, en los niños”*.

A continuación, dentro de las Políticas de Privacidad hay un apartado que se dirige a los usuarios internacionales, es decir, a todos aquellos que no residen ni tienen su domicilio en Estados Unidos:

“El Sitio y el Servicio WhatsApp se alojan en los Estados Unidos y están destinados y dirigida a los usuarios de Estados Unidos. Si usted es un usuario que accede al sitio y usa el servicio WhatsApp desde la Unión Europea, Asia o cualquier otra región de leyes y reglamentos que rigen la recogida de datos personales, uso y revelación, que difieren de las leyes de los Estados Unidos, por favor tenga en cuenta que el Sitio WhatsApp y sus servicios como esta Política de Privacidad y nuestros Términos de Servicio, se rigen por las leyes de California, que van a transferir su información personal a los Estados Unidos y que usted da su consentimiento expreso para la transferencia y el consentimiento a ser gobernados por la ley de California para estos fines”).

Es decir se fija la jurisdicción y la legislación de California para cualquier disputa que pueda haber entre un usuario y WhatsApp.

En los contratos internacionales es competente el tribunal que las partes hayan acordado, es la regla de la sumisión. La aplicación de la ley extranjera²⁰⁴, que las partes, en virtud de su autonomía, eligieron para regir sus obligaciones contractuales, puede estar limitada por razones de Orden Público o de Fraude a la Ley, según los principios de Derecho Internacional Privado. Estos límites juegan un rol especial en contratos que, por variadas razones, están sujetos a normas de orden público, como por ejemplo estatutos protectores de carácter imperativo en materia de contratos de adhesión²⁰⁵ (como en este caso, en donde la ley establece ciertos requisitos que deberán tener estos contratos como “*acceso claro, comprensible e inequívoco de las condiciones generales del mismo y la posibilidad de almacenarlos o imprimirlos*” Cuestión que a nuestro entender no se cumpliría, ya que, solo existe una versión en Inglés de los Términos de Servicio y Política de Privacidad en la página de WhatsApp Messenger, cuestión no menor porque difícilmente una persona que no sabe inglés pueda entender claramente lo que acepta, en ese punto, existe una responsabilidad de WhatsApp según el artículo 12 A de la Ley del Consumidor), contratos celebrados por consumidores y contratos de trabajo. Para el Prof. Ramírez Necochea, las partes pueden pactar libremente su contrato dentro de la esfera que les

²⁰⁴ Según nuestra ley la forma de hacer valer una sentencia dictada en el extranjero es por vía del exequátur, artículo 242 a 251 del Código de Procedimiento Civil.

²⁰⁵ La ley N° 19.496 que “Establece normas sobre protección de derechos de los derechos consumidores” señala en su artículo 12 A respecto a las obligaciones del proveedor que: “*En los contratos celebrados por medios electrónicos, y en aquéllos en que se aceptare una oferta realizada a través de catálogos, avisos o cualquiera otra forma de comunicación a distancia, el consentimiento no se entenderá formado si el consumidor no ha tenido previamente un acceso claro, comprensible e inequívoco de las condiciones generales del mismo y la posibilidad de almacenarlos o imprimirlos.*

La sola visita del sitio de Internet en el cual se ofrece el acceso a determinados servicios, no impone al consumidor obligación alguna, a menos que haya aceptado en forma inequívoca las condiciones ofrecidas por el proveedor.

Una vez perfeccionado el contrato, el proveedor estará obligado a enviar confirmación escrita del mismo. Ésta podrá ser enviada por vía electrónica o por cualquier medio de comunicación que garantice el debido y oportuno conocimiento del consumidor, el que se le indicará previamente. Dicha confirmación deberá contener una copia íntegra, clara y legible del contrato”.

da la autonomía de la voluntad, limitada por el Orden Público (En un país que se habla español, ¿no es contrario al orden publico un contrato de adhesión escrito netamente en inglés? Es contrario a la Ley N° 19.496) y el fraude a la ley. No hay ninguna limitación de someterse a un tribunal extranjero (electio fori) respecto de derechos disponibles en materia civil y comercial, de tal forma que procede la sumisión como regla general²⁰⁶.

A este respecto (lo que analizaremos no tomando en cuenta el aparente problema de existir solo una versión en inglés de los Términos de Servicio y Política de Privacidad de WhatsApp²⁰⁷) podemos señalar que; como los servidores de WhatsApp están en Estados Unidos y todos nuestros mensajes y archivos están en una base de datos en California, que es donde están las oficinas de WhatsApp, y que supuestamente no hay ningún servidor ni ninguna información de WhatsApp en Chile (salvo seguramente las que recogen los proveedores de servicio de internet móvil en Chile), efectivamente son las leyes de California las que van a regir lo que a base de datos respecta y derechos de autor²⁰⁸. Pero las transferencias de información se hacen con una persona que vive en Chile, residente en Chile, por tanto en cuanto a esa comunicación si podrán regir las leyes de nuestro país, inclusive nuestra legislación de protección a la vida privada Ley N 19.628°, sino se opone a las leyes de California, cuestión que resolverá en definitiva el tribunal competente de Santa

²⁰⁶ RAMÍREZ NECOCHEA, HÉCTOR. 2010. Curso Básico De Derecho Internacional Privado. Santiago de Chile, LegalPublishing Abeledo Perrot. 196p.

²⁰⁷ Durante el transcurso de este trabajo hicimos una solicitud a WhatsApp Messenger de enviarnos los Términos de Servicio y Política de Privacidad en idioma español, cuestión que hasta a fecha de presentación de este trabajo aún esperamos.

²⁰⁸ EE.UU. tiene leyes mucho más estrictas que Chile respecto a los derechos de autor, específicamente la *California Online Privacy Protection Act*, es una ley que protege la privacidad de los consumidores online residentes en California. Mal podría aplicársele a un extranjero que no reside en California.

Clara, California. En este sentido, además, tendrán aplicación las leyes y preceptos de los tribunales de Estados Unidos.

De todas maneras, **la información que realicemos a través de internet, pasa por los servidores de los proveedores de internet de nuestro país, en este sentido, a ellos si le es aplicable la Ley Sobre Protección de la Vida Privada N° 19628** que hemos analizado en este trabajo con detalle y la legislación de nuestro país al respecto, teniendo jurisdicción los tribunales competentes de nuestro país.

En el caso de que WhatsApp sea adquirida o se fusione con una tercera entidad, se reservan el derecho a transferir esa información. En el caso de insolvencia, bancarrota, reorganización, quiebra o cesión en beneficio de acreedores, o la aplicación de leyes o principios equitativos que afecten los derechos de los acreedores en general (que señalan que esperan sea poco probable y también lo esperan sus usuarios), no podrán controlar como esta información sea tratada, transferida o usada.

Finalmente respecto a los cambios y actualizaciones de esta Política de Privacidad, la empresa señala que es nuestra responsabilidad estar al tanto de las modificaciones que ella pueda sufrir. El uso continuado del Sitio y servicios WhatsApp constituye aceptación tácita de esta Política de Privacidad y sus enmiendas. Cuestión a la que ya hemos hecho referencia anteriormente.

A continuación analizaremos la Constitución de California respecto al derecho a la privacidad, pues es a la que se sujeta WhatsApp ante algún asunto contencioso en sus términos de servicio.

5.4.5 Constitución de California y el derecho a la privacidad

Establece en su artículo 1, sección 1 el derecho constitucional a la Privacidad, señalando que: *Todas las personas son por naturaleza libres e independientes y tienen derechos inalienables. Entre ellos están disfrutando la defensa de la vida y la libertad, adquirir, poseer y proteger propiedades, y la búsqueda y la obtención de la seguridad, la felicidad y la vida privada*²⁰⁹.

5.4.6 California Online Privacy Protection Act²¹⁰

En este apartado nos enfocaremos en explicar cuáles son las principales leyes de protección de la privacidad en línea u *online* del Estado de California, que son las

²⁰⁹ CALIFORNIA CONSTITUTION, ARTICLE N°1 DECLARATION OF RIGHTS, SECTION 1. All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy. CALIFORNIA, OFFICE OF PRIVACY PROTECTION. California Constitution. [en línea] <http://www.leginfo.ca.gov/.const/.article_1> [consulta: 09 septiembre 2014]

²¹⁰ Que se traduciría como “Ley de Protección de la Privacidad Online de California”.

que directamente nos interesan para referirnos a la legislación aplicable en este sentido a WhatsApp.

California tiene las siguientes leyes sobre Privacidad en línea²¹¹:

- *Anti-Phishing Act of 2005 - Código de Negocios y Profesiones, secciones 22948-22948.3: Esta ley prohíbe el "phishing", el acto de hacerse pasar por una empresa legítima o agencia gubernamental en un correo electrónico, página web o comunicación por Internet, a fin de engañar al destinatario para que revele su información personal.*
- *Computer Spyware - Código de Negocios y Profesiones, sección 22947 y siguientes: Esta ley prohíbe a una persona no autorizada, a sabiendas, de instalar o proporcionar software que realiza determinadas funciones, tales como tomar el control del ordenador o la recogida de información de carácter personal, en la computadora de otro usuario ubicadas en California.*
- *Cyberbullying - Código de Educación sección 32261: Esta ley define el acoso como uno o más actos de: acoso sexual, violencia por odio, acoso intencional, amenazas o intimidación, dirigido contra el personal del distrito escolar o alumnos, cometido por un alumno o grupo de alumnos. El acoso, incluyendo acoso cometido por medio de un acto electrónico,*

²¹¹CALIFORNIA, OFFICE OF PRIVACY PROTECTION. Privacy Laws. [en línea] <http://www.privacy.ca.gov/privacy_laws/index.shtml> [consulta: 09 septiembre 2014]

como se define, incluye un mensaje en un sitio web de redes sociales de Internet.

- *Personal Information Collected on Internet (Información Personal Recopilada en Internet) - Sección 11015.5 del Código de Gobierno: Esta ley se aplica a las agencias del gobierno estatal. Al recoger información personal por medios electrónicos, las agencias deben proporcionar ciertos avisos. Antes de compartir información de una persona con terceros, las agencias deben obtener el consentimiento escrito de la persona.*
- *Public Officials, Online Privacy (Funcionarios Públicos, Privacidad en Línea) - Código de Gobierno 6254,21: Esta ley prohíbe publicar o mostrar en Internet la dirección o el número de teléfono de cualquier funcionario electo o nombrado, como se define, si el funcionario ha hecho una solicitud por escrito a no revelar su información. Las entidades que reciban tal demanda deben quitar la información de inmediato y asegurarse de que no sea publicado.*
- *Reproductive Health Care, Online Privacy (Cuidado de Salud Reproductiva, Privacidad en línea) - Código de Gobierno, sección 6218 y siguientes: Esta ley protege la seguridad de los proveedores de salud, empleados, voluntarios, y los pacientes mediante la prohibición de la publicación de domicilio de cualquiera de esas personas, número de teléfono, o imagen en Internet, bajo circunstancias específicas.*

- *Safe at Home Participants, Online Privacy (Participantes de Casa Segura, Privacidad en Línea) - Código de Gobierno, secciones 6206,5 6206,7, 6215,3, 6208, 6215.4, 6215.7, 6208.1, 6208.2, y 6218,01: Esta ley proporciona a los participantes en el Programa de la Secretaría de Estado, Casa Segura, de la confidencialidad de las direcciones (para víctimas de violencia doméstica o acoso y proveedores de salud reproductiva, empleados y voluntarios) con el derecho de exigir la retirada si su información personal, incluida la dirección de su casa y el número de teléfono de los motores de búsqueda en línea o bases de datos, e impone obligaciones relacionadas a los operadores de motores de búsqueda y bases de datos.*
- *Online Privacy Protection Act of 2003 (Ley de Protección de la Privacidad Online de 2003) - Código de Negocios y Profesiones, secciones 22575-22579: Esta ley obliga a los operadores de sitios web comerciales o servicios en línea que recopilan información personal sobre **residentes** de California a través de un sitio web para publicar una política de privacidad visible en el sitio y para cumplir con su política. La política de privacidad debe, entre otras cosas, identificar las categorías de información personal obtenida de los visitantes del sitio y las categorías de terceros con los que el operador puede compartir la información. Un operador viola la presente ley al no publicar una política de Privacidad en un plazo de 30 días desde la notificación de incumplimiento, o si el operador ya sea a sabiendas, deliberadamente o por negligencia, materialmente no cumple con las disposiciones de su póliza. Esta ley entra en vigor en julio 1, 2004.*

Esta ley si establece ciertos requisitos que deberá cumplir un operador de un sitio web comercial, entre ellas la de publicar una política de privacidad en un plazo de 30 días desde la notificación de incumplimiento. Pero en lo que a mayor abundamiento respecta, solo lo obliga respecto de la información personal que recopile de residentes de California. Así que, en lo que respecta a personas no residentes, de otros estados y consecuentemente de otros países, esta ley no les es aplicable.

CAPITULO VI

GSMA

6.1 GSMA: La Asociación Profesional Global de la Industria Móvil

La GSMA es una organización de operadores móviles y compañías relacionadas que representa los intereses de los operadores móviles alrededor del mundo. La GSMA tiene representación en 220 países (entre ellos Chile), con casi 800 operadoras móviles en todo el mundo (entre ellas (Entel Chile, Movistar, Claro), y más de 200 empresas del amplio ecosistema móvil, que incluyen fabricantes de teléfonos, empresas de software, proveedores de equipamiento, empresas de internet y, medios de comunicación y empresas de entretenimiento²¹².

Los miembros de la GSMA representan a más de cinco mil millones de conexiones²¹³. *“La GSMA tiene un papel fundamental que jugar en el desarrollo de políticas públicas relacionadas con la industria móvil y sus clientes. Nuestro equipo de políticas públicas lidera de forma activa el debate político, representando a la*

²¹² En una de sus noticias telecom.com señalo que GSMA es *“una de las asociaciones comerciales más poderosas del mundo, que presiona a los Gobiernos en todo, desde la política fiscal a la estrategia de precios”*. TELECOMS. Michael O’HARA, Chief Marketing Officer, GSM Association. [en línea] <<http://www.telecoms.com/13386/michael-o%E2%80%99hara-chief-marketing-officer-gsm-association/>> [consulta: 09 septiembre 2014]

²¹³ La GSMA es una de las organizaciones más poderosas del mundo respecto a operadores de telefonía móvil y su influencia tanto en ella como en los países.

industria móvil ante gobiernos y reguladores y creando un ambiente regulatorio que maximice las oportunidades de desarrollo para los operadores móviles y los beneficios a largo plazo para los usuarios de dispositivos móviles”²¹⁴.

6.2 Móviles y Privacidad

En estos últimos años, GSMA se ha preocupado del Derecho a la Privacidad de los usuarios de telefonía móvil, planteando básicamente lo mismo que ya hemos podido apreciar en este trabajo: *“La convergencia de la industria móvil y de internet, combinada con el incremento de teléfonos inteligentes (“Smartphones”) y aplicaciones y servicios innovadores, está trayendo beneficios considerables a los clientes y a la sociedad. Estos avances, bien acogidos, están también reestructurando el paisaje de la privacidad en la red, llevando a nuevos retos de privacidad dentro del ecosistema móvil. Los enfoques tradicionales de la privacidad online se basan habitualmente en el cumplimiento de un mosaico de leyes nacionales y locales, allí donde existen. Sin embargo, las nuevas aplicaciones móviles, servicios y flujos de datos están creciendo de forma global y las leyes de protección de datos asociadas a una geografía no parece que puedan estar en consonancia con ese crecimiento. Los usuarios de móviles están buscando cada vez más un tratamiento consistente de su privacidad, independiente de las tecnologías, modelos de negocio y flujos de datos implicados y están buscando formas que les ayuden a administrar*

²¹⁴GSMA. Móviles y Privacidad. [en línea] <<http://www.gsma.com/latinamerica/wp-content/uploads/2012/07/Privacy-leaflet-2012-Spanish.pdf>> [consulta: 09 septiembre 2014].

*su privacidad. Un reto clave para la industria es encontrar formas dentro del contexto móvil, de ayudar a los usuarios a tomar decisiones informadas sobre su información y su privacidad. Otro reto clave es asegurar que la privacidad del usuario sea respetada y protegida por todos aquellos que diseñan y construyen nuevos servicios y aplicaciones”*²¹⁵.

Lo anterior ha significado la creación de una serie de principios que se han manifestado en directrices por parte de GSMA a las más de 800 operadoras móviles que representa, en cuanto a la privacidad y el tratamiento de datos personales.

6.3 Cuáles son los datos personales según la GSMA²¹⁶

GSMA, sin ánimos, como ellos dicen, de reinterpretar la ley, señalan lo que se debe entender cuando se habla de datos personales de los usuarios (“*usuario final del dispositivo móvil que inicia el uso de una aplicación o servicio, y que puede o no puede ser el "cliente" de una aplicación o un proveedor de servicios*”²¹⁷) de telefonía móvil. La información personal puede incluir:

- a) datos recopilados directamente del usuario, por medio de una interfaz de usuario de la aplicación (nombre, dirección, fecha de nacimiento);

²¹⁵ GSMA. "Móviles y Privacidad". op. cit.

²¹⁶GSMA. Mobile Privacy Principles. [en línea] <<http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacyprinciples20121.pdf>> [consulta: 09 septiembre 2014]. p.5

²¹⁷GSMA. Mobile Privacy Principles. op. cit., p. 5

- b) datos reunidos indirectamente tales como el número de teléfono, el IMEI o el UDID;
- c) datos recopilados acerca del comportamiento, tales como datos de localización, historial de navegación o aplicaciones usadas, que están asociados a un perfil único y;
- d) datos generados por el usuario, tales como listas de contactos, vídeos y fotos, mensajes, emails, notas y registros de llamadas.

6.4 Directrices respecto al almacenamiento de datos y privacidad

GSMA plantea que puede haber seguridad sin privacidad, pero no puede haber privacidad sin seguridad, en esta línea se dirige a las operadoras en una serie de interrogantes que ellas deberán hacerse para entender mejor como mejorar la seguridad de los datos personales de sus usuarios: *“Piense por qué necesita retener la información personal de un usuario y por cuánto tiempo necesita tenerla almacenada, ¿puede justificarlo? La información personal almacenada indefinidamente pierde valor con el paso del tiempo, pero incrementa su coste y su riesgo. Identifique por cuánto tiempo es necesaria (por contraposición a deseable) una información personal determinada para su modelo de negocio y asegúrese de eliminarla de forma segura cuando ya no sea requerida. Establecer periodos de almacenamiento para sus datos (tan breves como sea posible) es una buena decisión*

de negocio, puede ayudarle a controlar riesgos y costes y a evitar acciones de los reguladores o publicidad negativa si algo saliera mal (porque la almacenó por demasiado tiempo y los datos fueron puestos en peligro)”.

A continuación GSMA entrega a los miembros de su organización 4 directrices respecto al almacenamiento de datos personales, su ejecución, a lo que suma casos prácticos y ejemplos al respecto²¹⁸:

DIRECTRIZ	EJECUCIÓN	CASOS PRÁCTICOS Y EJEMPLOS
<p>DIRECTRIZ 1</p> <p>Administración activa de los identificadores.</p> <p>Siempre que una aplicación cree o use un identificador único, tome medidas para asegurarse de que el identificador está asociado al usuario legítimo de la aplicación y mantenga esta información actualizada.</p>	<p>Cada una de las partes que usa identificadores es responsable de tomar medidas para:</p> <ul style="list-style-type: none"> • asegurarse de que un identificador único se asocia con un usuario único • asegurarse de que los identificadores únicos se almacenan actualizados y sólo por el tiempo necesario para cumplir con los propósitos y razones notificadas a los usuarios • evitar que un identificador único se asocie con otro 	<p>Las operadoras móviles pueden reasignar identificadores tales como MSISDN (números móviles) a otros clientes sin que la aplicación lo sepa. Si usted capta el MSISDN de un usuario debe tomar medidas para asegurarse de que esa información es correcta y está actualizada mediante confirmaciones periódicas con el usuario.</p> <p>Asimismo, los fabricantes de dispositivos deben asignar un Identificador Único de Dispositivo (UDID). Los usuarios</p>

²¹⁸GSMA. Directrices para el diseño de privacidad en el desarrollo de aplicaciones. [en línea] <<http://www.gsma.com/latinamerica/wp-content/uploads/2012/07/Privacy-Guidelines-Spanish-booklet-20120613-LR.pdf>> [consulta: 09 septiembre 2014]. p.10-12

	<p>usuario a no ser que sea necesario por una necesidad de negocio justificada (Ver Casos prácticos y ejemplos)</p>	<p>de móvil pueden reemplazar su teléfono móvil y venderlo a otros individuos. A no ser que se tenga cuidado, el nuevo propietario del móvil podría estar fácilmente asociado con el Identificador Único de Dispositivo u otros identificadores únicos asociados con el dueño anterior. Esta asociación y vínculo podría tener consecuencias en las experiencias de privacidad en la red del nuevo usuario y en su utilización del dispositivo. Cada una de las partes que recopila y usa UDIDs es responsable de asegurar que se cumple con esta directriz.</p>
<p>DIRECTRIZ 2 Mantenga la información protegida. Tome las medidas apropiadas para proteger la información personal del usuario de accesos o revelaciones no deseados.</p>	<p>Tome medidas técnicas y decisiones de negocio que eviten la mala utilización o alteración de la información personal. Siempre que una aplicación cree o recopile información personal considerada confidencial, como datos de acceso, UDIDs, números de móvil, datos de contacto, información financiera... esa</p>	<p>Recopilar y guardar cierta información cuando es sencillamente innecesario crea el riesgo de que se pierda, sea robada y mal utilizada. Si necesita recopilar, transmitir y retener información confidencial como pueden ser los datos de pago de un usuario o sus datos de acceso, deberá hacer esta información segura mediante encriptación o un mecanismo adecuado de función</p>

	información debe ser guardada y transmitida de forma segura	hash y borrar esa información cuando ya no sea necesaria.
<p>DIRECTRIZ 3</p> <p>Autentique allí donde las medidas de seguridad lo exijan.</p> <p>Autentique a los usuarios siempre que sea posible usando métodos de autenticación ajustados a los riesgos.</p>	<p>Siempre que la reafirmación de la identidad del mundo real sea un componente importante de un servicio, se deberá desarrollar una autenticación más sofisticada, como la autenticación de dos factores usando un teléfono móvil y UICC.</p> <p>Considere la utilización de CAPTCHAs y RE-CAPTCHAs para poder diferenciar miembros genuinos de aquellos que sólo generan spam. Use las herramientas técnicas para restringir el spidering (o araña web) y las descargas colectivas o el acceso sin el permiso de la red.</p>	
<p>DIRECTRIZ 4</p> <p>Fije periodos de almacenamiento y eliminación.</p> <p>La información personal que se va a guardar debe</p>	<p>Justifique la recopilación y almacenamiento de información personal de acuerdo con necesidades de negocio claramente identificadas u obligaciones</p>	<p>Los datos almacenados en un perfil de conducta relacionados con un usuario único por medio de cookies u otro identificador de dispositivo, incluso si no existe otra información identificable, no</p>

<p>estar sujeta a periodos de almacenamiento y eliminación, justificados por necesidades de negocio claramente identificadas u obligaciones legales.</p>	<p>legales. Fije una política de actuación y aplíquela a nivel técnico y de procesos de negocio.</p> <p>Una vez que la información personal ya no es necesaria para cumplir con un objetivo de negocio específico y legítimo o con requerimientos/obligaciones legales, debe ser destruida o pasar a ser anónima.</p> <p>Los datos verdaderamente anónimos pueden ser almacenados indefinidamente. Para convertir una serie de datos en anónimos, elimine cualquier información que pueda servir para identificar a un individuo en concreto, asegurándose de que no es posible identificar a ese individuo de nuevo y asegurándose de que esos datos no pueden relacionarse, por medio de identificadores únicos, con un individuo específico no identificado</p>	<p>deben ser considerados realmente anónimos. Un perfil con el identificador único eliminado o hacheado puede considerarse anónimo</p>
--	--	--

CONCLUSIONES

El avance de la tecnología sin duda alguna ha traído a los hombres nuevos y difíciles desafíos que ha debido enfrentar en cada oportunidad con una mente clara y agudos sentidos. El desarrollo de la telefonía móvil ha sido uno de los logros más grandes y a la vez de los más difíciles retos que ha tenido que enfrentar la humanidad. Esta disyuntiva se debe precisamente al sino de la tecnología en general, ya que todo avance de ella significa mejoras en la calidad de vida y a la vez riesgos a ella. La pregunta que en este sentido se nos presenta es ¿cómo eliminar, o al menos, minimizar estos riesgos? La respuesta es clara, a través de un sistema normativo firme que prevea estos y les dé solución, y a la vez la creación de un sistema fiscalizador firme que vele por la correcta observación y respeto por estas normas.

La telefonía móvil ha tenido un rápido crecimiento en los últimos 50 años, y en definitiva sus mayores avances los ha alcanzado en la última década. La creación de los llamados “Smartphone” o “teléfonos inteligentes” cambiaron los paradigmas de las comunicaciones, al establecer que el teléfono ya no solo servía para comunicarse,

sino para realizar casi cualquier tarea que nos propusiéramos. Vital en este desarrollo han sido los sistemas operativos como hemos visto, y como han logrado entregar al usuario a través de una interfaz amigable y simple, mayores y mejores rendimientos de su teléfono móvil, lo que también ha contribuido a que se creen nuevas y mejores tecnologías para nuestros celulares. Es el caso de las llamadas aplicaciones, software o programas livianos que han permitido hacer casi cualquier cosa con nuestro móvil, y de las cuales existen millones de ellas, cada una diferente a la otra, cada una con un objetivo distinto a la anterior. Con estas .app, que es la extensión por el cual se identifican estas aplicaciones, uno puede ver televisión, jugar, predecir temblores, aprender a hacer un nudo de corbata, bajar de peso, reparar un computador, etcétera, todo al alcance de la mano, todo al alcance de un bolsillo.

Y como hemos señalado, en este magnífico desarrollo, también han aparecido los riesgos de su uso. Nosotros nos hemos enfocado en los riesgos que el avance de la telefonía móvil, con los llamados Smartphone, ha significado para la privacidad. De esta manera hemos visto como nuestra Constitución Política de la Republica se interesa en la protección de ciertos derechos que considera fundamentales en las personas, y los ha garantizado a través del artículo 19 de ella. En este artículo que consta de 26 numerales, el legislador se ha preocupado del derecho a la privacidad

en dos de ellos, el N° 4 y N°5, de los cuales a nosotros nos compete el primero. Este artículo 19 N° 4 es la base legislativa para el planteamiento legal de la privacidad al establecer “*El respeto y protección a la vida privada y a la honra de la persona y su familia*”. Y aunque a la redacción de este artículo ni siquiera se preveían los avances de la tecnología en el mundo de la informática, su sentido es claro y preciso al poner en rango constitucional la protección de este derecho. Así también la Constitución en su artículo 20°, entrega a las personas respecto de este derecho la acción de protección, para restablecer y garantizar el imperio del derecho cuando este se vea privado, perturbado o amenazado.

Sin embargo lo anterior, nuestro sistema normativo ha establecido una ley especial en la protección a la vida privada, preocupándose mayormente del tema, o al menos queriendo hacerlo, aunque la Ley no regule todos los aspectos que debería regular en ella, respecto a la vida privada. Hablamos precisamente de la Ley N° 19.628 que se titula “Sobre la Protección de la Vida Privada” y que se subtitula “Protección de Datos de Carácter Personal”. En ella, como hemos visto, se pretende entregar protección a la vida privada limitándola al área de la protección de datos personales, específicamente en el campo de acción de los banco de datos que puedan manejar privados o terceros respecto de las personas. El derecho de acceso y control

de la información por parte de los individuos, se instrumentaliza procesalmente en el denominado Habeas Data, una acción especial destinada a encausar procesalmente la libertad informática y la protección de los datos personales, constituyéndose en un eficaz instrumento en la protección de la vida privada, conciliando el debido respeto a la garantía constitucional con el derecho de ejercicio de la actividad de quienes se dedican a procesar información personal, a través de banco o base de datos.

Con todo, la Ley N° 19.628 está lejos de ser perfecta, ya que primeramente, entre sus líneas limita la protección de la vida privada a un solo aspecto de ella, la protección de datos personales, tal vez, incluso sin prever los avances en el área informática. Además, no establece la creación de un registro público de base de datos, pues, solo los organismos públicos que manejen base de datos deberán registrarse pero no así los privados. No crea un organismo administrativo regulador idóneo para el funcionamiento de las bases de datos. No se da la obligación de informar previamente por parte del responsable de una base de datos, al titular de los datos respecto de cuales se pretende efectuar un tratamiento, ya que, se establece que la información es pública. No se fijan medidas de seguridad concreta en el tratamiento de datos respecto de las filtraciones que puedan suceder. El no haber

prohibido la transferencia internacional de datos personales a terceros países que no dispusiesen de un adecuado sistema de protección de datos, etcétera.

Todo lo anterior cobra mucho sentido cuando lo analizamos a la luz de la tecnología móvil, en relación a algunas aplicaciones que permiten la comunicación a través de dos o más personas, como es el caso de WhatsApp Messenger. Vimos como a través de esta aplicación, las personas que utilizaran este servicio podían comunicarse a través de mensajería equivalente a SMS con un formato chat. Explicamos cómo esta información debía pasar primeramente por los servidores de WhatsApp en California EE.UU. y como WhatsApp a través de sus Términos de Servicio y Política de Privacidad, establecía la jurisdicción a los tribunales de este California en caso de cualquier conflicto entre usuarios y terceros afectados con él. Mencionamos en este sentido, el artículo 1 sección 1 de la Constitución de California que asegura y protege el derecho de perseguir y proteger la privacidad, que la ley encargada de regular los bancos de datos de WhatsApp sería la *California Online Privacy Protection Act*, una ley mucho más específica que nuestra Ley N° 19.628, al referirse directamente a la protección de la privacidad online, pero que solo se aplica a los residentes del Estado de California.

Sin embargo lo anterior, por el uso del internet móvil que hacemos, algunos de nuestros datos llegan a los servidores de nuestros proveedores de telefonía móvil, y en este caso ellos si están sujetos a la legislación de nuestro país, concretamente a la Ley N° 19.628 y consecuentemente a nuestra jurisdicción.

También existe una responsabilidad de WhatsApp a los ojos de la Ley N° 19.496 en cuanto el artículo 12 A señala que en los contratos (de adhesión) celebrados por medios electrónicos, el consentimiento no se entenderá formado si el consumidor no ha tenido previamente un acceso claro, comprensible e inequívoco de las condiciones generales del mismo. Cuestión que se viola toda vez que WhatsApp solo tiene un documento en su página web de los Términos de Servicio y Políticas de Privacidad en idioma inglés, la misma que se muestra al instalar la aplicación, sin tener una versión en idioma español, lo que la hace claramente incomprensible para aquellos que no tiene porque necesariamente manejar el idioma inglés, en un producto que está destinado a todo el mundo (aunque en principio haya sido solo para los estados unidos). Al año 2011 WhatsApp tenía 100 millones de usuarios en todo el mundo, la última modificación de sus Términos de Servicio y Políticas de Privacidad la realizo en 7 de julio del 2012, momento en el que ya estaba al tanto de la masificación de su producto, por el cual en todo el mundo pagaban, sin tener al

menos la más mínima diligencia de mantener una versión en otros idiomas de ellos, como si lo han hecho servicios como Google o Facebook, las cuales tienen sus principales oficinas en California, EE.UU.

La tecnología es necesaria y de eso no cabe duda, su desarrollo implica evolución y los avances necesarios para enfrenar el presente y el futuro de la humanidad, sin embargo, ésta debe hacerse acompañada de una normativa fuerte y consistente que regule sus aplicaciones. De esta manera, y aún no de la mejor manera, nuestra normativa si proporciona los instrumentos necesarios para que los individuos puedan protegerse de la mala utilización por terceros extraños de su información que no es consentida, y aun la que si cuenta con su permiso, procurando evitar que la publicación y mala utilización de su información personal pueda significarnos pasar un mal rato, y más aún, conllevar un serio e importante perjuicio, no solo para nuestras vidas, sino también para nuestros padres, esposa, esposo e hijos.

BIBLIOGRAFÍA

A) Fuentes Bibliográficas Impresas

- ÁLVAREZ, RODRIGO. 2002. Análisis del régimen jurídico de protección de datos de carácter personal. Memoria de prueba para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile, Facultad de Derecho. 183p.
- ANGUITA RAMÍREZ, PEDRO. 2007. La protección de datos personales y el derecho a la vida privada: Régimen jurídico, jurisprudencia y derecho comparado. Santiago de Chile, Editorial Jurídica de Chile. 627p.
- ARRIETA, RAÚL. 2009. Chile y la protección de datos personales: ¿están en crisis nuestros derechos fundamentales? Santiago de Chile, Ediciones Universidad Diego Portales.

- CORTE SUPREMA, CORTE DE APELACIONES DE SANTIAGO. 1993. Informe Comisión Interamericana de Derechos Humanos: Sentencia caso Martorell, Rol N°983-93, 15.06.1993. Revista de Derecho y Jurisprudencia, Tomo XC (2), sección 5ta.
- DRUMMOND, VÍCTOR. 2004. Internet, Privacidad y Datos personales. Madrid, España, editorial Reus S.A., 181p.
- GUZMÁN ERRAZURIZ, JAIME. Actas oficiales de la comisión constituyente. Tomo IV (129), 12 de junio de 1975.
- HERNANDEZ, ANA. y PALACIOS, JUAN. 2008. El dato sensible: su tratamiento en Chile y en el derecho comparado. Memoria de prueba para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile, Facultad de Derecho.
- JIJENA LEIVA, RENATO. 1992. Chile, la protección penal de la intimidad y el delito informático. Santiago de Chile, editorial Jurídica de Chile. 225p.
- NOGUEIRA ALCALÁ, HUMBERTO. 2002. El derecho a la libertad de opinión e información y sus límites: honra y vida privada. Santiago de Chile, Universidad de Talca y Lexis Nexis. 385p.

- NOVOA MONREAL, EDUARDO. 1997. Derecho a la vida privada y la libertad de información: Un conflicto de derechos. 5ª ed. Santiago de Chile, siglo veintiuno editores. 224p.
- PARADA, BÁRBARA. 2008. El régimen de responsabilidad civil en la protección de datos personales en Chile. Memoria de prueba para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile, Facultad de Derecho. 192p.
- RAMÍREZ NECOCHEA, HÉCTOR. 2010. Curso Básico De Derecho Internacional Privado. Santiago de Chile, LegalPublishing Abeledo Perrot. 196p.
- WARREN, SAMUEL. y BRANDEIS, LOUIS. 1995. El derecho a la intimidad. Madrid, Civitas. 70p.

B) Fuentes Bibliográficas Electrónicas

- ANDROID. 2012. Discover Android. [en línea]
<<http://www.android.com/about/>> [consulta: 22 enero 2015]
- APRENDERAPROGRAMAR. Qué Es Un Servidor y Cuáles Son Los Principales Tipos De Servidores (proxy, Dns, Web, Ftp, Smtplib...). [en línea]
<http://www.aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftpsmtplib-&catid=57:herramientas-informaticas&Itemid=179> [consulta: 09 septiembre 2014].
- AREATECNOLOGIA. Telefonía Móvil. [en línea]
<<http://www.areatecnologia.com/telefoniamovil.htm>> [consulta: 22 enero 2015]
- BARRÍA, SUSANA. 2007. Webmóvil: desarrollo de soporte comunicacional web a través de dispositivos de telefonía móvil [en línea]

<http://www.tesis.uchile.cl/tesis/uchile/2007/barria_s/html/index-frames.html> [consulta: 22 enero 2015]

- **BASOALTO, REBOLLEDO.** 2007. Administración de mensajería de texto en cascada para teléfonos celulares [en línea] <http://www.tesis.uchile.cl/tesis/uchile/2007/basoalto_cr/html/index-frames.html> [consulta: 22 enero 2015]
- **BASTERRETICHE, JUAN.** 2007. Dispositivos Móviles. [en línea] <<http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/tfbasterretiche.pdf>> [consulta: 15 diciembre 2014]
- **BIBLIOGRAFIASYVIDA.** Alexander Graham Bell. [en línea] <<http://www.biografiasyvidas.com/biografia/b/bell.htm>> [consulta: 15 diciembre 2014]
- **BIBLIOTECA DEL CONGRESO NACIONAL.** Actas oficiales de la comisión constituyente. [en línea] <http://www.bcn.cl/xbc3x/lc/cpolitica/constitucion_politica/Actas_comision_ortuzar/Tomo_IV_Comision_Ortuzar.pdf> [consulta: 15 diciembre 2014]

- BIBLIOTECA DEL CONGRESO NACIONAL. 2012 Spam. [en línea] <http://www.bcn.cl/leyfacil/recurso?item_id=4840&leng=es> [consulta: 09 septiembre 2014].
- CABEZAS, LOGAN. y MOYA, FERNANDO. 2008. El derecho al anonimato del usuario de internet. Memoria de prueba para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile, Facultad de Derecho. [en línea] <http://www.tesis.uchile.cl/tesis/uchile/2008/cabezas_p/html/index-frames.html> [consulta: 15 diciembre2014]
- CALIFORNIA, OFFICE OF PRIVACY PROTECTION. California Constitution. [en línea] <http://www.leginfo.ca.gov/const/.article_1> [consulta: 09 septiembre 2014]
- CALIFORNIA, OFFICE OF PRIVACY PROTECTION. Privacy Laws. [en línea] <http://www.privacy.ca.gov/privacy_laws/index.shtml> [consulta: 09 septiembre 2014]
- CEDI 2015. Académicos. [en línea] <<http://www.derecho.uchile.cl/centro-de-estudios-en-derecho-informatico/quienes-somos/88570/academicos>> [acceso: 22 enero 2015].

- CELARE. 2011. La Protección de Datos en la Unión Europea y América Latina. [en línea] EUROLAT: Revista de Relaciones Eurolatinoamericanas. Vol.17(83)

<<http://eulacfoundation.org/sites/eulacfoundation.org/files/pdf/LA%20PROTECCION%20DE%20DATOS%20EN%20LA%20UE%20Y%20AL.pdf>> [consulta: 22 enero 2015]
- CLARÍN. 2012. Einstein, lleno de culpa por la bomba atómica. [en línea]

<<http://edant.clarin.com/diario/2005/07/04/sociedad/s-03601.htm>> [consulta: 09 septiembre 2014]
- CORRAL TALCIANI, HÉRNAN. 2000. Configuración Jurídica del Derecho a la Privacidad II: Concepto y Delimitación. [en línea] Revista Chilena de Derecho, Vol. 27 N°2, p.331-355, Sección Estudios. 2000.

<<https://corraltalciani.files.wordpress.com/2010/04/configuracion-juridica-del-derecho-ii.pdf>> [consulta: 22 enero 2015]
- DE BERNARDO, CESAR. y PRIEDE, TIZIANA. Marketing Móvil, una nueva herramienta de Comunicación: Análisis y nuevas perspectivas para el mercado español. [en línea], España, Editorial Netbiblo

<<https://books.google.cl/books?id=4nz1NoSYiaUC&pg=PA2&lpg=PA2&dq>

=historia+de+la+telefon%C3%ADa+m%C3%B3vil+bell+laboratories&source=bl&ots=oPaeTNSvwt&sig=3XjZudF3THXvlp4nZHTYzmpNot0&hl=es&sa=X&ei=zyPIVL6VHNW0sQSgroKgBQ&ved=0CDwQ6AEwBQ#v=onepage&q=historia%20de%20la%20telefon%C3%ADa%20m%C3%B3vil%20bell%20laboratories&f=false> [consulta: 22 enero 2015]

- DIARIO LA NACIÓN. Presentan El Primer Celular con Android, el software de Google. [en línea] <<http://www.lanacion.com.ar/1052747-presentan-el-primer-celular-con-android-el-software-de-google>> [consulta: 22 enero 2015].
- DIARIO EL PAÍS. 1992. Raymond Lindon, pionero del derecho de Prensa. [en línea] El País Archivo. 30 de enero, 1992. <http://elpais.com/diario/1992/01/30/agenda/696726001_850215.html> [consulta: 22 de enero 2015]
- DURÁN, LUIS. 2004. Régimen jurídico general de las telecomunicaciones y convergencia. Memoria de prueba para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile, Facultad de Derecho. [en línea] <http://www.tesis.uchile.cl/tesis/uchile/2004/duran_1/html/index-frames.html> [consulta: 22 enero 2015]

- EDITORIAL JURIDICA DE CHILE. 1982. Revista de derecho y jurisprudencia y gaceta de los tribunales. [en línea] Santiago de Chile, Editorial Jurídica de Chile.
 <<http://books.google.cl/books?id=J112rgulunAC&printsec=frontcover#v=onepage&q&f=false>> [consulta: 01 diciembre 2014]
- EMOL. 2012 Robo de información y ataques a smartphones marcaron los problemas informáticos del 2012. [en línea]
 <<http://www.emol.com/noticias/tecnologia/2012/12/28/576743/robo-de-informacion-y-ataques-a-smartphones-marcaron-los-problemas-informaticos-del-2012.html>> [consulta: 22 enero 2015]
- EMOL. 2014. WhatsApp habría habilitado “doble check” para mensajes leídos. [en línea]
 <<http://www.emol.com/noticias/tecnologia/2014/11/05/688549/whatsapp-habria-habilitado-un-doble-check-azul-para-avisar-cuando-un-mensaje-fue-leido.html>> [consulta: 22 enero 2015]
- GALLARDO, RODRIGO. El Derecho de Acceso a la Información Frente a la Protección de Datos Personales. Memoria de prueba para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile,

Facultad de Derecho. [en línea]

<http://tesis.uchile.cl/bitstream/handle/2250/111389/de-gallardo_r.pdf?sequence=1> [consulta: 22 enero 2015]

- GSMA. Móviles y Privacidad. [en línea]

<<http://www.gsma.com/latinamerica/wp-content/uploads/2012/07/Privacy-leaflet-2012-Spanish.pdf>> [consulta: 09 septiembre 2014]

- GSMA. Mobile Privacy Principles. [en línea]

<<http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacyprinciples20121.pdf>> [consulta: 09 septiembre 2014]

- GSMA. Directrices para el diseño de privacidad en el desarrollo de aplicaciones. [en línea] <<http://www.gsma.com/latinamerica/wp-content/uploads/2012/07/Privacy-Guidelines-Spanish-booklet-20120613-LR.pdf>> [consulta: 09 septiembre 2014]

- IETF. 2000. Mecanismo que permite la comunicación segura entre servidor y cliente. Microsoft: 'Using Digest Authentication as a SASL Mechanism. [en línea] <<http://www.ietf.org/rfc/rfc2831.txt>> [consulta: 22 enero 2015].
- JIJENA. [en línea] <<http://www.jijena.com/>> [acceso: 22 enero 2015].

- LÓPEZ, NICOLÁS. 2011. Efecto de las redes de cuarta generación (LTE) en los servicios móviles en Chile. [en línea] <http://www.tesis.uchile.cl/bitstream/handle/2250/104136/cf-lopez_nm.pdf?sequence=3> [consulta: 22 enero 2015]
- MARTINES, P., CABELLO, M. y DÍAZ MARTÍN, J. 1997. Sistemas Operativos: teoría y práctica. [en línea] <<https://books.google.es/books?id=wXzwFPaVku0C&printsec=frontcover&dq=SISTEMAS+OPERATIVOS+Y+TEORIA+PRACTICA&hl=es&sa=X&ei=ChTLVKXsIrWJsQTfgYLYCQ&ved=0CCIQ6AEwAA#v=onepage&q=SISTEMAS%20OPERATIVOS%20Y%20TEORIA%20PRACTICA&f=false>> [consulta: 22 enero 2015]
- OECD. Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. [en línea] <<http://www.oecd.org/internet/interneteconomy/15590267.pdf>> [consulta: 15 diciembre 2014]
- ORTIZ PABÓN, HÉCTOR. 2005. Sistemas Operativos Modernos. [en línea] <http://books.google.es/books?id=3Hb6f3gyCxUC&pg=PA11&hl=es&source=gbp_toc_r&cad=3#v=onepage&q&f=false> [consulta: 22 enero 2015]

- QUIMINET. 2011. ¿Cómo funciona el teléfono celular? [en línea] <<http://www.quiminet.com/articulos/como-funciona-el-telefono-celular-2571317.htm>> [consulta: 22 enero 2015]
- RADIOCOMUNICACIONES.NET. Historia de la Telefonía Móvil. [en línea] <<http://www.radiocomunicaciones.net/telefonía-movil.html>> [consulta: 22 enero 2015]
- ROA N., MATÍAS. 2013. Facebook frente al derecho a la vida privada y la protección de datos personales. Memoria de prueba para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile, Facultad de Derecho. [en línea] <http://www.tesis.uchile.cl/bitstream/handle/2250/113249/de-roa_m.pdf?sequence=1> [consulta: 22 enero 2015]
- SECURITY BY DEFAULT. 2011. WhatsApp y Su Seguridad, ¿pwn3d? [en línea] <<http://www.securitybydefault.com/2011/03/whatsapp-y-su-seguridad-pwn3d.html>> [consulta: 22 enero 2015]
- SLIDESHARE. 2012. Historia de la telefonía celular. [en línea] <<http://www.slideshare.net/javitojr/historia-de-la-telefonía-celular-12598330>> [consulta: 22 enero 2015]

- SUAREZ CROTHERS, CHRISTIAN. 2000. El concepto de derecho a la vida privada en el derecho anglosajón y europeo. [en línea] <http://mingaonline.uach.cl/scielo.php?script=sci_arttext&pid=S0718-09502000000100010&lng=es&nrm=iso p.103-120> [consulta: 15 diciembre 2014]
- TELECOMS. Michael O'HARA, Chief Marketing Officer, GSM Association. [en línea] <<http://www.telecoms.com/13386/michael-o%E2%80%99hara-chief-marketing-officer-gsm-association/>> [consulta: 09 septiembre 2014]
- TELEFONOS-MOVILES. Martin Cooper - El Inventor De Los Teléfonos Móviles. [en línea] <<http://www.telefonos-moviles.com/articles/item.asp?ID=24>> [consulta: 06 septiembre 2014]
- UNION EUROPEA. Introducción Coordinada De Un Sistema De Comunicaciones Móviles e Inalámbricas De Tercera Generación (UMTS) En La Comunidad. [en línea] <http://europa.eu/legislation_summaries/other/l24202_es.htm> [consulta: 22 septiembre 2014]
- WAYERLESS. 2014. WhatsApp marca un nuevo récord a dos meses de su compra por Facebook. [en línea]

<<https://www.wayerless.com/2014/04/whatsapp-ya-tiene-500-millones-de-usuarios-activos/>> [consulta: 22 enero 2015]

- WHATSAPP. 2015. WhatsApp FAQ - ¿Es gratis enviar mensajes WhatsApp? [en línea] <<http://www.whatsapp.com/faq/es/general/20965922>> [consulta: 22 enero 2015].
- WHATSAPP. 2015. WhatsApp FAQ - ¿Por qué me pide el número de teléfono y acceso a mi lista de contactos? [en línea] <*WhatsApp.com* <<http://www.whatsapp.com/faq/es/general/20971813>> [consulta: 22 enero 2015].
- WHATSAPP. 2015. ¿Qué significan los ticks al lado de mis mensajes? [en línea] <<https://www.whatsapp.com/faq/es/general/20951546>> [consulta: 22 enero 2015]
- WHATSAPP. 2015. WhatsApp: Legal. [en línea] <<http://www.whatsapp.com/legal/#Privacy>> [consulta: 22 enero 2015].
- WHATSAPP. 2015. Información legal de WhatsApp. [en línea] <<https://www.whatsapp.com/legal/>> [consulta: 22 enero 2015]

- WIKIPEDIA. Sistema Telefónico Móvil Avanzado. [en línea]
 <http://es.wikipedia.org/wiki/Sistema_Telef%C3%B3nico_M%C3%B3vil_Avanzado> [consulta: 22 enero 2015]
- WIKIPEDIA. Telefonía móvil. [en línea]
 <http://es.wikipedia.org/wiki/Telefon%C3%ADa_m%C3%B3vil#Conexi.C3.B3n_a_Internet> [consulta: 22 enero 2015]
- XATAKA MÓVIL. 2012. Nokia y el cada vez más oscuro futuro de Symbia.
 [en línea] <<http://www.xatakamovil.com/nokia/nokia-y-el-cada-vez-mas-oscuero-futuro-de-symbian>> [consulta: 22 enero 2015]
- XATAKA MÓVIL. 2012 Seguridad usando Whatsapp: Lo estás haciendo mal.
 [en línea] <<http://www.xatakamovil.com/seguridad/seguridad-en-whatsapp-lo-estas-haciendo-mal>> [consulta: 22 enero 2015]
- XATAKA MÓVIL. T-MOBILE G1. [en línea]
 <<http://www.xataka.com/moviles/tmobile-g1>> [consulta: 22 enero 2015].
- ZONATRADE. Celulares. [en línea]
 <<http://www.zonatrade.com/Celulares/Celulares.htm>> [consulta: 22 enero 2015]

E) Fuentes Bibliográficas consistentes en Revistas o Artículos en Revistas

- BARROS, ENRIQUE. 1998. Honra, privacidad e información: un crucial conflicto de bienes jurídicos. Revista de Derecho, Universidad Católica del Norte, año 5: 45-58.
- FIGUEROA, RODOLFO. 2013. El derecho a la privacidad en la jurisdicción de protección. Revista Chilena de Derecho, 40 (3): 859-889