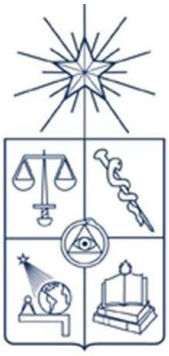

UNIVERSIDAD DE CHILE

FACULTAD DE DERECHO

DEPARTAMENTO DE DERECHO PROCESAL

CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO

“DON’T BE EVIL”

GOOGLE Y PRIVACIDAD

Memoria para optar al título de Licenciada en Ciencias Jurídicas Y Sociales

RAYEN CAMPUSANO BARRA

Profesor Guía Daniel Álvarez Valenzuela

Santiago de Chile

Agosto de 2014

omnia mutantur

nos et mutamur in illis

TABLA DE CONTENIDOS

CAPITULO I. VIDA PRIVADA..... 10

1. Fundamentación de la privacidad..... 11

2. Concepto..... 13

3. Regulación normativa 17

4. Características de la vida privada..... 18

5. Contenido y protección de la vida privada..... 20

6. Titular del derecho a la vida privada..... 23

6.1 Persona Natural..... 23

6.2 Persona Fallecida 24

6.3 Personas Jurídicas..... 25

7. Limitaciones al derecho a la vida privada 27

7.1 Limitaciones de carácter general..... 28

7.2 Limitaciones de carácter personal 29

8. Colisión con otros derechos..... 32

9. Responsabilidad..... 33

CAPITULO II. DATOS PERSONALES..... 37

1. Historia de la Ley 19.628 39

2. Estructura 41

3. Ámbito de aplicación..... 42

4. Conceptos importantes..... 43

4.1. Dato personal 43

4.2. Dato sensible..... 44

4.3. Dato estadístico..... 45

4.4. Titular de datos..... 45

4.5. Registro o banco de datos..... 47

4.6. Responsable del registro o banco de datos..... 47

4.7. Tratamiento de datos 48

4.8. Comunicación o transmisión de datos..... 49

4.9. Almacenamiento de datos..... 49

4.10. Fuentes accesibles al público..... 49

4.11. Procedimiento de disociación de datos..... 50

5. Hipótesis del tratamiento debido de datos..... 50

5.1. Titular consiente expresamente en ello 50
5.2. Autorización de la Ley 19.628 51
5.3. Otras disposiciones legales 52
6. Hipótesis de tratamiento especiales 52
6.1. Datos sensibles 52
6.2. Obligaciones de carácter económico, financiero, bancario o comercial. 53
7. Principios relativos al tratamiento de datos personales 53
7.1. Principio de libertad en el tratamiento de datos personales 54
7.2. Principio de información y consentimiento del titular 54
7.2.1. Fuente accesible al público 55
7.2.2. Tratamiento por personas jurídicas privadas 57
7.2.3. Tratamiento por organismos públicos 57
7.3. Principio de finalidad: uso conforme al fin 59
7.4. Principio de calidad 60
7.5. Principio de protección especial a los datos sensibles 61
7.6. Principio de seguridad de los datos 62
7.7. Principio de responsabilidad o deber de secreto 63
7.8. Garantías ante la transmisión de datos 64
8. Autodeterminación Informativa: derechos del titular de datos personales 66
8.1. Derecho a la información y acceso 66
8.2. Derecho de modificación o rectificación 67
8.3. Derecho de cancelación 68
8.4. Derecho de bloqueo 69
8.5. Derecho a obtener copia 69
9. Derechos y obligaciones del titular del registro. 70
10. Mecanismos de control 70
10. 1 Mecanismos de autocontrol 72
10. 2 Mecanismos de heterocontrol 73
11. Responsabilidad 75
12. Critica a la legislación nacional 76
13. El dilema del consentimiento 83
CAPÍTULO III. GOOGLE 88
1. Descripción general 92

1.1. Productos de búsqueda 92
1.2. Productos para comunicar, mostrar y compartir 93
1.3. Productos para el celular 94
2. Poder de la información 94
3. Principales productos y posible afectación privacidad 101
3.1. Buscador Google 101
3.2. Google Chrome 105
3.3. Gmail 110
3.4. Youtube 113
3.5. Servicios de Publicidad 115
3.6. Android 117
3.7. Google + ... 120
3.8. Street View 121
4. Políticas de Privacidad 124
4.1. Datos recogidos por Google 125
4.2. Utilización de los datos recogidos 128
4.3. Acceso a los datos personales y actualizaciones 130
4.4. Datos personales compartidos por el usuario 131
4.5. Datos personales compartidos por Google 131
4.6. Seguridad de los datos 133
4.7. Aplicación 135
4.8. Cumplimiento 135
4.9. Modificaciones 136
5. Condiciones de uso de los productos y servicios de Google 137
6. Problemáticas en la Política de Privacidad y Condiciones de Uso de los productos de Google que afectan el derecho a la privacidad. 142
7. Consagración jurisprudencial del "Derecho al olvido". Sentencia del Tribunal de Justicia Europeo 154
CONCLUSIONES 160
BIBLIOGRAFÍA 166

INTRODUCCIÓN

La información es poder. El manejo de datos personales a través de las tecnologías digitales permite transformar información parcial y dispersa en un conjunto de datos organizados disponibles para consulta y tratamiento masivo desde casi cualquier lugar del mundo.

La nueva fuente de poder unida a la brecha informática y el desconocimiento de los riesgos en la utilización de tecnologías acrecienta las posibilidades de afectar el derecho a la privacidad.

Actualmente no nos percatamos con claridad de la importancia y el valor de los datos personales entregados en Internet e incluso desconocemos el tratamiento que de ellos se hace.

Entre sus múltiples funcionalidades, Google es el más poderoso motor de búsqueda en la actualidad. Millones de usuarios lo utilizan y por lo mismo puede imponer nuevas reglas en la web. Desde su creación, cualquier tipo de información es accesible, de forma libre y bajo el eslogan corporativo “don’t be evil”[1], enfocado a la no utilización de datos con fines maliciosos.

[1] GOOGLE EMPRESA. Lo que creemos. Puedes hacer dinero sin hacer el mal [en línea] <https://www.google.cl/intl/es-419/about/company/philosophy/> [consulta: 05 junio 2014]

Desde el año 2012 en adelante, esta gran empresa ha modificado y actualizado su política de privacidad, con la intención de mostrar resultados de búsqueda y anuncios más relevantes para el usuario, ayudándolo a conectarse con la gente o acelerar y facilitar el compartir información. Ha unificado los términos de uso de sus distintos servicios en uno solo para hacerlo más fácil y entendible al usuario, y con la intención de crear un único perfil almacenado por Google. La idea es mejorar los resultados de búsqueda que se realizan y recibir anuncios u ofertas más ajustados y aproximados a los gustos y preferencias de la persona que lo utiliza.

¿Pero, qué significa esto? Principalmente que toda la información y datos personales que circulan en los distintos servicios como gmail, youtube, picasa, google earth, maps, calendar, docs, blogger, google +, incluso en noticias, imágenes, libros, sitios y grupos relacionados con la plataforma, Os Android, y el propio motor de búsquedas de Google están agrupados en una sola base de datos.

En términos simples, Google sabe quiénes somos, quiénes nos rodean, qué cosas nos gustan o disgustan, cuáles son nuestras preferencias, dónde estamos, a dónde vamos y hasta cómo lucimos físicamente: una gran cantidad de información reunida en un solo lugar.

La privacidad ya no se aplica en un sentido puramente negativo de rechazar la intromisión a la vida privada, en no permitir la difusión de datos personales o en no participar de la vida social.[2] Ahora podemos entenderlo en un sentido positivo, como afirmación de la propia libertad y dignidad de la persona, es decir, como la limitación impuesta por el individuo sobre el poder informático y como el control activo del medio y el fin de este.

La autodeterminación informativa consiste en la libertad de determinar quién, qué y con qué ocasión pueden conocerse informaciones concernientes a una persona determinada. La libertad informática implica la posibilidad de consentir o no los usos que se puedan realizar de los datos personales. El derecho a la autodeterminación informativa es equivalente a la libertad informática cuya función es garantizar a los ciudadanos facultades de información, acceso y control de los datos personales que les conciernen.

Al aceptar los términos de uso de un servicio sin saber, aceptamos el tratamiento de datos personales sin estar conscientes del contenido y alcance de este, ni quienes podrán acceder a ello. Google puede compartir estos datos personales con terceros administradores de dominio en la instalación de aplicaciones, para el tratamiento externo a filiales o terceros de confianza, o por motivos legales cuando Google considera de “buena fe” que existe una

[2] Véase: BANDA Vergara, Alfonso. 2000. Manejo de datos personales, un límite al derecho a la vida privada. Universidad Austral de Chile. 59 p.

necesidad razonable de acceder a los datos personales, utilizarlos, conservarlos o reservarlos.[3]

Los datos recogidos por Google se obtienen mediante la información que nosotros mismos entregamos en el registro, y por medio de datos obtenidos de la utilización de sus servicios. El peligro de vulneración a nuestra vida privada es grande y el control de la información que posee Google, importante. Por lo que cabe preguntarse si las políticas de privacidad de Google se adecuan o no a los estándares de protección de la vida privada en Chile.

¿Cómo podemos estar seguros que el tratamiento de datos es debido? ¿La justificación de mejorar el servicio es un fin legítimo para unificar toda la información personal existente en los distintos servicios de Google? ¿Pueden organismos estatales solicitar y recibir información personal de un usuario? ¿Personas físicas ajenas pueden obtener nuestros datos?

Para responder estas preguntas, es necesario analizar, por un lado, la normativa sobre protección de la vida privada de las personas en la Constitución Política de la República, tratados internaciones sobre derechos humanos y la Ley 19.628 sobre Protección de Datos Personales; y por otro lado, la nueva política de privacidad de Google y las condiciones del servicio.

[3] GOOGLE. Política de Privacidad. Información que compartimos. [en línea] <https://www.google.cl/intl/es-419/policies/privacy/#infosharing> [consulta: 05 junio 2014]

En el capítulo número uno se expondrá acerca del derecho a la vida privada, analizando cuál es su fundamentación, concepto, regulación normativa, características, contenido, titulares, limitaciones y el sistema de responsabilidad.

En el capítulo número dos se estudiará la ley 19.628, revisando su historia, estructura, aplicación, conceptos, hipótesis de tratamiento, principios, derechos y obligaciones del titular del registro, sistema de responsabilidad, para finalizar realizando una crítica a la legislación nacional reconociéndola como insuficiente y poco efectiva, además de mencionar el dilema del consentimiento que cuestiona el control significativo que las personas tienen sobre sus datos.

En el capítulo número tres analizaremos a Google, realizando una descripción general, cuál es su rol en la era de la información, cuáles son sus principales productos y cómo afectan a la privacidad, sus políticas y condiciones de uso y las problemáticas que traen aparejadas. Finalizando con la sentencia del Tribunal de Justicia Europeo que consagra el derecho al olvido en Internet.

Esta investigación pretende ser un aporte al estudio del derecho fundamental a la privacidad y alarma frente a una posible vulneración de derechos producida por la plataforma más utilizada de internet, Google.

CAPITULO I. VIDA PRIVADA

La era de la tecnología y en especial de la informática, ha traído como consecuencia una serie de problemáticas de orden jurídico, en especial en temas de privacidad, por cuanto existe un mayor acceso a la información de forma sistemática y centralizada en bases de datos que pueden contener elementos privados que no se quiere sean conocidos por la mayoría de la población.

"Si bien el hombre es un ser que por sus limitaciones individuales y su capacidad de comunicación precisa de la vida de relación, posee también una esfera de vida íntima, propia y familiar, respecto de la cual es soberano para decidir si la comparte o no con los demás, ámbito que debe ser respetado como algo inviolable".[4]

El avance tecnológico que está experimentando la sociedad requiere de un sistema normativo adecuado y actualizado, que se amolde a las nuevas tecnologías y respete los derechos fundamentales consagrados en nuestra Constitución Política (en adelante, CPR) y Tratados Internacionales (en adelante, TTII), sin imponer limitaciones que eviten el progreso ni restrinjan el

[4] MEINS Olivares Eduardo. 2000. Derecho a la Intimidad y a la Honra en Chile. Año/ Vol. 6, Nº 001. Talca Chile. Universidad de Talca. Ius et Praxis. 308 p.

uso de nuevas herramientas sino que entreguen mecanismos idóneos y adecuados que impidan el uso indebido y abusivo de la tecnología.

1. Fundamentación de la privacidad

Siguiendo al filósofo alemán Spaemann, analizado por Corral Talciani[5], creemos que la fundamentación del derecho a la privacidad es antropológica, entendiendo que la dignidad humana es un derecho fundamental que se reconoce y descubre en el mismo y todo ser humano, como un fin en sí y relacionado en sociedad.

Los derechos no son concesiones de ningún poder o convención de aquellos que los gozan sino que emanan de todo hombre por el único hecho de pertenecer a la especie humana, por lo que siempre existirá un mínimo de dignidad de la cual el hombre no puede ser desposeído.

La vida de relación es un elemento esencial de la naturaleza humana porque el hombre no solo vive integrado de una comunidad sino que no puede realizar su existencia sin una red compleja y múltiple de innumerables relaciones interpersonales y multipersonales que le proporcionan el sustento

[5]CORRAL Talciani, Hernán. 2000. Configuración Jurídica del Derecho a la Privacidad I: Origen, desarrollo y fundamentos. Vol. 27 Nº 1. Chile. Revista Chilena de Derecho. Selección Estudios. 51 – 79 p.

necesario para desarrollarse de manera digna. En palabras de Javier Hervada "la persona siendo individuo, es más que eso, es un ser-en-relación, justamente porque, en virtud de su riqueza ontológica, es capaz de abrirse a los demás, de expandirse, en la alteridad, o sea, permaneciendo en ella misma"[6]

La dignidad humana entendida como ese fin en sí mismo que hace absoluto el valor del ser humano, y la relacionalidad de su naturaleza que lo presenta siempre como un ser "con otro", constituye la explicación más comprensiva y coherente con la pretensión de proteger y potenciar un espacio específico llamado vida privada.

"La vida privada como bien jurídico, y el derecho a que ella sea respetada, lejos de construirse bajo la imagen de un sujeto de derechos que busca la soledad y que lo dejen en paz, puede y debe explicarse sobre la base de un sujeto de derechos que en su esencial dignidad necesita relacionarse con sus semejantes y requiere para desarrollar relaciones satisfactorias y vínculos autorrealizadores de la posibilidad de llevarlos a cabo sin que sea sometidos a la vigilancia o control de terceros ajenos a ella."[7]

[6] HERVADA, Javier. 1993. Los derechos inherentes a la dignidad de la persona humana. En Escritos de Derecho Natural. 2º Edición. Pamplona. EUNSA. 681 p.
[7] CORRAL Talciani, Hernán. 2000. Configuración Jurídica del Derecho a la Privacidad… op cit nota Nº 5. 78 p.

Los gobiernos deben evitar inmiscuirse en espacios de privacidad que requieren las distintas relaciones que permiten al individuo desarrollar su personalidad, pero al mismo tiempo deben procurar velar porque confluyan armónicamente y no se conviertan en mecanismos de control y de utilización de un individuo en contra de otro. “El rol del Estado es insustituible en la labor de propender a que las relaciones a través de las cuales se organiza la sociedad tiendan, o al menos, no dañen el bien de la comunidad.”[8]

En esta visión antropológica hay que entender que el derecho a la vida privada debe ser de la persona más que del individuo, por cuanto la persona posee de individualidad pero es al mismo tiempo, social, abierta y receptiva a los demás. El hombre no es un solitario sino más bien un comunicador y la intimidad es la condición necesaria de la sociabilidad del hombre.

2. Concepto

El concepto de vida privada no es fácil de establecer ni delimitar por cuanto su acepción cambia dependiendo del país, nivel socioeconómico e incluso entre una persona y otra.[9] Además, no existe acuerdo doctrinal a nivel nacional y comparado acerca de su definición ni contenido, por lo que urge la

[8]Ibídem
[9]MEINS Olivares Eduardo. 2000. Derecho a la Intimidad… op cit nota Nº4. 304 p.

necesidad de un desarrollo jurisprudencial uniforme que abarque la realidad antropológica y jurídica de nuestro país.

Por otro lado, la doctrina nacional alude indistintamente a la intimidad, privacidad y vida privada. Si bien la expresión “privacidad” es más amplia que el término “intimidad”, y revela mejor el bien jurídico a proteger que la expresión de “vida privada”, para esta presentación se usarán indistintamente estos conceptos, por cuando bien pueden utilizarse como expresiones intercambiables ya que la distinción carece de efectos jurídicos en nuestro ordenamiento.[10]

Siguiendo las definiciones de Diccionario de la Real Academia Española, privacidad es el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión. Intimidad es la zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia. Enunciaciones que a nuestro parecer son incompletas porque giran en torno al secreto y confidencialidad sin tomar en cuenta “la idea de control que la propia persona ejerce respecto de su información”.[11]

[10] En tal sentido: JIJENA LEIVA, RENATO JAVIER. Chile, La Protección Penal de la Intimidad y el Delito Informático.1992. Editorial jurídica de Chile. Santiago de Chile. 1º edición.
[11] MEINS Olivares Eduardo. 2000. Derecho a la Intimidad… op cit nota Nº4. 304 p.

Vial propone: “El derecho a la vida privada se podría definir como aquel derecho que está destinado a proteger la dignidad y libertad humana, por medio del reconocimiento a su titular de un poder de control sobre su ámbito privado, que en su núcleo central se identifica con el cuerpo y la afectividad, y respecto la información relativa a persona.” [12]

Barros sigue la postura de Charles Fried, quien define el derecho a la privacidad como un control que tenemos sobre la información acerca de nosotros mismos:

“La privacidad expresa un poder para excluir a personas no autorizadas del conocimiento de hechos que quedan bajo el control exclusivo de cada cual. Para ello la privacidad establece dos limitaciones conexas entre sí, pero diferentes. Por un lado, este ámbito de privacidad impide que terceros se introduzcan, por cualquier medio, en ámbitos físicos de intimidad, y por otro, que se difundan hechos relativos a un ámbito concebido como privado.”[13]

Corral Talciani ofrece su concepto de privacidad como bien jurídico: “es la posición de una persona (o entidad colectiva personal) en virtud del cual se encuentra libre de intromisiones o difusiones cognoscitivas de hechos que

[12] VIAL Solar, Tomás. 2000. Hacia la construcción de un concepto constitucional del derecho a la vida privada. Volumen XVI Nº3. Chile. Revista Persona y Sociedad. 68 p.
[13] BARROS Bourie, Enrique. 1998. Honra, privacidad e información: un crucial conflicto de bienes jurídicos. Año 5- 1998. Coquimbo. Revista de Derecho, Universidad Católica del Norte Sede Coquimbo, 46 p.

pertenecen a su interioridad corporal y psicológica o a las relaciones que ella mantiene o ha mantenido con otros, por parte de agentes externos que, sobre la base de una valoración media razonable, son ajenos al contenido y finalidad de dicha interioridad o relaciones.[14]

El fundamento de la protección a la vida privada de la persona es la dignidad del ser humano y el libre desarrollo de la personalidad del individuo.[15] "El derecho a la intimidad habilita a su titular para rechazar cualquier intromisión sobre aquel ámbito de su vida privada que es inaccesible a los demás si no es bajo su explícito consentimiento."[16]

Este derecho fundamental es una doble garantía, por un lado, la persona no va a ser objeto de intromisiones en su vida privada -los que lo hagan deberán responder-, y por el otro lado, implica una garantía de preservación de la intimidad, entendiéndola como la total disponibilidad sobre el ámbito de lo íntimo, sin interferencias o impedimentos. El derecho a la intimidad "no sólo es el poder de resistencia a una intromisión ilegítima, sino también la potestad de controlar el flujo de información que pueda circular en el escenario público".[17]

[14]CORRAL Talciani, Hernán. 2000. Configuración jurídica del derecho a la privacidad II: concepto y delimitación. Volumen 27 Nº 5. Chile. Revista Chilena de Derecho, Sección Estudios. 347 p.
[15] En este sentido: sentencias del Tribunal Constitucional 2454-13, 2513-13, 2422-13.
[16] CARILLO, Marc. 2003. El derecho a no ser molestado. Información y vida privada. Navarra: Colección Divulgación Jurídica. Thomson Aranzadi. 15 p.
[17] CARILLO, Marc. 2003. El derecho a… op. cit. nota Nº 16. 15 p.

3. Regulación normativa

El artículo 19 Nº 4 de la CPR establece "El respeto y protección a la vida privada[18] y a la honra de la persona y su familia"[19] como una fórmula que elevó el derecho a la intimidad como garantía constitucionalmente protegida para ser respetada horizontalmente tanto por entes gubernamentales como privados.

El reconocimiento constitucional del derecho a la vida privada "se enmarca en un modelo de Estado que tiene a las personas y a los grupos en los que se integra como sujetos básicos de derechos".[20] La Comisión de estudios de la Nueva Constitución (en adelante, CENC) determinó que el derecho del artículo 19 Nº 4 es un principio general sin contenido específico, derecho subjetivo que no reconoce fuentes directas sino sólo valores a proteger.[21]

Por su lado la Convención Americana de Derechos Humanos, en su artículo 11 establece:

[18] Previamente, es necesario señalar que en términos de esta presentación se analizará solo el respeto a la vida privada, dejando de lado el respeto a la honra de la persona, por ser derechos que se relacionan pero no son lo mismo y su análisis debe ser apartado.
[19] CHILE. Ministerio Secretaría General de la Presidencia. Decreto 100. Fija el texto refundido, coordinado y sistematizado de la Constitución Política de la República de Chile. 22 de septiembre del 2005.
[20] CARILLO, Marc. 2003. El derecho a… op. cit. nota Nº 16. 30 p.
[21] Historia de la Ley. Constitución Política De La República de Chile de 1980. Artículo 19 N° 4. El Derecho A La Privacidad. 23 p.

“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.”

4. Características de la vida privada

La privacidad emana de la dignidad humana -con la que mantiene una relación sustancial, clara y directa- por lo que merece un reconocimiento y protección excepcionalmente categórica. La primacía axiológica del ser humano es el fundamento de la vida privada. Su respeto y protección son la base esencial para el desarrollo de la personalidad de cada individuo, así como su

manifestación en la colectividad a través de grupos intermedios con los que se estructura la sociedad.

Barros expone que la vida privada involucra dos aspectos, la privacidad como un límite a la indagación y a la privacidad como secreto:

Respecto de la primera, se refiere a que el derecho a la privacidad es "establecer límites a la manera como se obtiene información acerca de la forma de vida de las personas, inclinaciones o aspectos íntimos"[22], es decir una defensa frente al espionaje de la vida privada. Es ilícita la intrusión al ámbito personal (hogar, trabajo, correspondencia, entre otros espacios íntimos), mediante cualquier instrumento técnico, aunque nada se diga, publique o archive. Sin embargo, a veces, la limitación del espacio físico puede ser sutil o confusa como cuando se produce una instancia privada en un lugar público (ej. conversación privada en la calle).

El segundo aspecto engloba "la pretensión que todos tenemos de que ciertos hechos relativos a nuestras vidas ordinarias y a nuestras inclinaciones y particularmente nuestras debilidades físicas o morales, no puedan ser objeto de conocimiento por terceros."[23] Resulta indiferente la verdad o falsedad de los hechos que son objeto de información. Lo que se pretende es el secreto, la

[22] BARROS. 1998. Honra, privacidad... op. cit. nota Nº 13. 46 p.
[23] BARROS. 1998. Honra, privacidad… op. cit. nota Nº13. 46 p.

divulgación de un hecho verdadero, por el solo hecho de afectar la privacidad, resultaría ilícito. Así también, basta que se afecte la autoestima o le cause simplemente un serio embarazo, ni siquiera que afecte su prestigio o vida de relación. Lo importante es el valor del secreto.

5. Contenido y protección de la vida privada

La Comisión de Estudios de la Constitución de 1980 cuyos trabajos se encuentran publicados en las Actas Oficiales de la Comisión Constituyente en las sesiones 128, 129 y 130, al intentar delimitar el concepto de vida privada creyeron indispensable que debe ser la jurisprudencia la que vaya calibrando y precisando en quién y hasta dónde alcanza el derecho a la privacidad.[24]

Es difícil establecer líneas precisas en un concepto mutable, por tanto frente a un caso concreto en que se vulnere el derecho, "es el tribunal respectivo a quien compete decidir si la faceta de la vida de la persona que se estime afectada queda o no comprendida dentro del ámbito del derecho a la intimidad". [25]

[24] Historia de la Ley. Constitución Política De La República de Chile de 1980… op cit nota Nº 21. 24 p.
[25] MEINS Olivares Eduardo. 2000. Derecho a la Intimidad… op cit nota Nº4. 305 p.

El problema es que en nuestro país la jurisprudencia nacional ha sido tardía, poco sistemática y no se ha hecho cargo completamente de la realidad que regula el artículo 19 Nº 4.

Teniendo en cuenta tales circunstancias, hay aspectos que deben ser considerados dentro de la protección de este derecho fundamental:

El propio cuerpo[26]: nos referimos a hechos o actos efectuados por la persona en forma reservada respecto de su espacio corporal.

La salud de una persona o los miembros de su familia es considerado un dato sensible que debe ser protegido, especialmente si su conocimiento menoscaba a la persona dentro de su círculo personal, social o profesional.

En otros países se ha relacionado el aborto con la intimidad como un derecho de la mujer de decidir sobre el propio cuerpo frente a si desea o no procrear. “El Tribunal Supremo de Estados Unidos ha considerado que la interrupción del embarazo es una cuestión privativa de la mujer, entendida como una proyección de su derecho a la inviolabilidad de su vida privada.”[27]

[26] N. d. A. No nos referimos en este punto al derecho a la integridad corporal.
[27] MEINS Olivares Eduardo. 2000. Derecho a la Intimidad… op cit nota Nº4. 305 p.

Las ideas, creencias y pensamientos pertenecen a la vida privada de una persona sin importar si son de índole religioso, filosófico, político o de cualquier otro tipo. Este derecho está consagrado en el art. 19 Nº 6 y Nº 12 de la CPR.

Vida pasada: pertenece a la esfera privada de una persona si es motivo de agobio para ella, ya que se tiene derecho a olvidar hechos o situaciones bochornosas que no se quiere sean conocidas por otros.

Vida doméstica: dentro del hogar la persona tiene derecho a estar tranquila y no ser molestada. Si bien este derecho está consagrado en el art. 19 Nº 5 como la inviolabilidad del hogar, parte de la doctrina ha establecido que el fundamento del derecho se encuentra en la intimidad.

Familia: engloba los asuntos relacionados con el matrimonio, la intimidad con la pareja, vida sexual, relación con los hijos, paternidad, por nombrar algunos aspectos.

Comunicaciones: es un derecho de todas las personas, sea este epistolar, telegráficos, telefónicos, fax o cualquier forma de comunicación privada. Incluso se sanciona a quien difunda tales conversaciones, documentos o instrumentos. Está consagrado en el art. 19 Nº 5 de la CPR.

Situación económica personal: la intromisión y publicación maliciosa de datos de carácter económico puede causar un grave daño personal, familiar o profesional, especialmente si este es incorrecto o desactualizado.

Actos o situaciones privadas que se producen en lugares públicos: estos pueden ser conocidos por alguien y divulgados porque pierden el concepto de privados dado el espacio donde se produce. Existiría un consentimiento tácito para la intromisión de terceros. Sin embargo, para calificar un hecho como privado o público, no solo debe considerarse el espacio donde se realiza sino además si los intervinientes han adoptado las debidas seguridades para mantener su reserva.

6. Titular del derecho a la vida privada

6.1 Persona Natural

Es titular del derecho a la vida privada todo individuo de la especie humana, cualquiera sea su edad, sexo, estirpe, condición socioeconómica, etc. Sin embargo, hay personas que en atención a la actividad que desarrollan o a su propio consentimiento permiten una disminución a su derecho a la privacidad.

El fundamento de la disminución de la privacidad de las autoridades gubernamentales y políticos es el interés público, por cuanto algunos asuntos de la vida personal de la persona pueden incidir en sus actividades públicas.[28]

Los actores, deportistas o gente de farándula son personas que voluntariamente se exponen a la publicidad, consistiendo que aspectos de su vida privada sea de dominio público, por lo que no es legítimo que posteriormente reclamen intromisión indebida.[29]

6.2 Persona Fallecida

Sobre el derecho a la privacidad de las personas fallecidas, existen dos posiciones diferentes. La jurisprudencia norteamericana entiende que éste se extingue con la muerte y el criterio europeo afirma que la privacidad de las personas fallecidas está igualmente protegido que la de las personas vivas, no obstante que de alguna manera el derecho disminuye a medida que se aleja en el tiempo de la muerte de la persona.

Alberto Lyon cree que "la privacidad de las personas fallecidas no protege los intereses de esa misma individualidad que ya no existe sino la de

[28] CORRAL Talciani, Hernán. 2001. La vida privada y la propia imagen como objetos de disposición negocial. Chile. Revista Chilena de Derecho, Universidad Católica del Norte, Nº8. 5p.
[29] MEINS Olivares Eduardo. 2000. Derecho a la Intimidad… op cit nota Nº4. 311 p.

aquellos que se encontraron ligados a ella por vínculos de sangre o parentesco que deben ser definidos por la legislación común".[30]

"La muerte extingue los derechos de la personalidad, pero su memoria constituye una extensión o prolongación de la personalidad que debe ser tutelada por el ordenamiento jurídico como bien jurídico digno de protección. Fallecido el titular del derecho y extinguida su personalidad civil, nos parece que su familia y sus herederos pueden invocar legitimación activa para su defensa, como asimismo las instituciones que tienen por fin proyectar su memoria."[31]

6.3 Personas Jurídicas

Respecto de la protección a la vida privada de las personas jurídicas, el alcance de la ley Nº 19.628 sobre protección de la vida privada, se refiere sólo las personas naturales, puesto que así se concibió en la idea matriz del proyecto que dio origen a la legislación, excluyendo así del ámbito de la ley a las personas jurídicas. Esta situación reporta un grave perjuicio en el tratamiento de sus antecedentes económicos y financieros, puesto que una interpretación restringida de la norma, deja fuera de los beneficios y procedimiento a todas las entidades de esta naturaleza.

[30] LYON Puelma, Alberto. 1993. Teoría de la personalidad. Chile. Ediciones Universidad Católica de Chile. 95 p.
[31] Nogueira Alcalá, Humberto. 2007. El derecho a la propia imagen como derecho fundamental implícito. fundamentación y caracterización. Chile. Revista Ius et Praxis, 13 (2): 245-285. 275 p.

Es por ello que una moción de la Cámara de Diputados establecida en el Boletín Nº 2422-07, creyó indispensable establecer normas sobre protección de la información de las personas jurídicas:

"El espíritu del legislador al aprobar la ley Nº 19.628, sobre protección a la vida privada, ha sido garantizar los derechos de todos quienes han visto atropelladas sus garantías producto del vacío legal que existía respecto al tratamiento de la información de las personas, como asimismo de los datos de carácter comercial, económicos o financieros. Por ello, es de toda justicia que los derechos y procedimientos de que gozan los titulares, como personas naturales, en el tratamiento de su información administrada en las bases de datos, sean extendidos también a las personas jurídicas, cual es el motivo de la presente iniciativa legal."[32]

Sin embargo, está moción ésta aún está en trámite y no se ha avanzado, dándonos a entender que no existe un ánimo serio de legislar al respecto.

El 23 de julio del 2011 se extendió la aplicación de protección de las personas jurídicas en lo concerniente a la predicción o evaluación de riesgo comercial que no esté basada en información objetiva.[33] No obstante omite

[32] CHILE. Tramitación de Proyectos Congreso Nacional.1999. Boletín 2422-07.
[33] CHILE. Ministerio Secretaría General de la Presidencia. 1999. Ley 19.628: Sobre protección de la vida privada. Modificado por la ley 20.521, del 23 de julio de 2011. Art. 9 inciso 3.

normativa expresa que garantice titularidad del derecho a la vida privada a las personas jurídicas. El hecho que el derecho de protección a la vida privada se halle enlazado con atributos humanos no obsta para excluir su aplicación a las personas jurídicas.

7. Limitaciones al derecho a la vida privada

Para penetrar en el ámbito reservado de la vida privada es necesario el consentimiento del titular del derecho o decisión de autoridad fundada en la ley, dictada conforme a la CPR. En todos los otros casos, la intromisión acarrea responsabilidad e indemnización de perjuicios.

El derecho a la vida privada admite restricciones que guarden la debida relación con el ordenamiento jurídico. Estas son excepcionales y solo se justifican en razón de la finalidad para las que han sido establecidas. Hay limitaciones de carácter general y limitaciones fundadas en la condición particular de algunas personas:

7.1 Limitaciones de carácter general

Frente a una guerra o una emergencia nacional se justificaría una limitación del derecho a la privacidad de las personas permitiendo una mayor facultad investigadora por parte del Estado como justificación de la seguridad del Estado.[34]

En periodos de normalidad institucional se autoriza la limitación frente a la investigación de un delito, donde se puede permitir el allanamiento de un hogar o la retención, apertura y registro de correspondencia.[35]

Las personas deben declarar y pagar determinados tributos e impuestos, entregando información personal económica a diversas entidades gubernamentales, en post del bienestar general de la sociedad.

Puede limitarse el derecho a la privacidad frente a la preocupación por la salud pública, como se da en el caso de algunas enfermedades contagiosas riesgosas para la población como el SIDA, Meningitis, entre otros.

[34] MEINS Olivares, Eduardo. 2000. Derecho a la Intimidad… op cit nota Nº4. 317 p.
[35] Díaz Tolosa, Regina. 2007. Delitos que Vulneran la Intimidad de las Personas: Análisis crítico del artículo 161-A del Código Penal Chileno. Chile. Revista Ius et Praxis, 13 (1): 291 – 314.

La investigación de filiación está relacionada con el ejercicio de derechos por parte de terceros y se permite la limitación frente al derecho a la identidad de la persona y el interés superior del niño.

La libertad de expresión comprende el derecho a dar y recibir información. Frente al conflicto con la vida privada debe ponderarse el interés público de la publicación[36]. El bien jurídico de la comunidad debe primar sobre el bien individual.

7.2 Limitaciones de carácter personal

Hay personas que en razón a su profesión, oficio o cargo se encuentran en el escenario público y el grado de derecho a la intimidad que puedan reclamar es mucho menor que el de una persona anónima

Razones de orden público justifican que aspectos de la privacidad de una persona sean revelados y se exija su publicidad (como por ejemplo personas que trabajan en el gobierno y se le exige actuar de cierta forma). Debemos ser conscientes entonces que, en ocasiones, el ámbito privado queda influido por la constante penetración de lo público. La garantía no es obstáculo para aquello

[36] En este sentido: LOVERA Parmo, Domingo. El Interés Público Como Estándar. Libertad De Expresión Y Vida Privada. Universidad Diego Portales. [en línea] <http://www.derechoshumanos.udp.cl/wp-content/uploads/2009/07/interes-publico.pdf> [consulta: 09 junio 2014] p. 95

que es de interés público salga a la luz. Algunos temas, en atención a su contenido e interés deben ser difundidos.

"El situarse libre y voluntariamente como persona de relevancia pública le hace soportar a una persona un mayor nivel de afectación o injerencia en su honra, asumiendo tal riesgo, ya que la divulgación de tal información de relevancia pública contribuye a la formación de opinión pública, obteniendo su máxima intensidad o eficacia justificadora frente al derecho al honor, ya que ello es necesario debido al pluralismo político, la conformación de un espíritu crítico y tolerante, sin los cuales se vacía de contenido la sociedad democrática y el control y fiscalización de las autoridades que actúan en representación del pueblo"[37]

La Corte de Apelaciones de Santiago[38], citando a la tratadista Angela Vivanco, expresa que "lo el público tiene derecho a conocer es aquello que tiene "interés público", que se ha transformado en el gran paradigma informativo de las sociedades contemporáneas y que se puede definir tanto objetiva como subjetivamente. Lo primero está en relación con la importancia de los hechos en sí y la conveniencia o necesidad de su conocimiento. Lo subjetivo está determinado por el sujeto de la información en cuanto específicamente es o no

[37] NOGUEIRA, Humberto. El Derecho a la Información en el Ámbito del Derecho Constitucional Chileno y Comparado en Iberoamérica y Estados Unidos. 1981. 74 p.
[38] Recurso de protección 10944-2011, de 22 de noviembre del 2011.

una persona de relevancia pública o una figura pública, lo que implica determinar la importancia que la persona a la que se refiere la noticia ostenta en la sociedad en la que esta se va a difundir.”

La Corte Interamericana de Derechos humanos en el caso de “Fontevecchia y D’Amico en contra de la República Argentina”, sentencia de 29 de noviembre de 2011, expresa que la protección a la vida privada disminuye en la medida de la importancia que puedan tener las actividades y funciones que ejerce la persona. El hecho de poseer un cargo político es aceptar voluntariamente un mayor escrutinio público pues el umbral no solo se asienta en la calidad del sujeto, sino en el interés público de las actividades que realiza.

La Corte señala que para resolver el conflicto entre el derecho a la vida privada de un alto funcionario público y el derecho a la libertad de expresión, es necesario verificar si realmente se produjo un daño cierto sobre el derecho afectado, dentro de un contexto que debe ser analizado por el juez, y que la información dada a conocer sea de relevancia pública.

La información sobre un funcionario es de relevancia pública cuando: a) a pesar de tener un componente de vida privada, tiene que ver con las funciones que esa persona ejecuta; b) se refiere al incumplimiento de un deber legal como ciudadano; c) resulta un dato relevante sobre la confianza

depositada en él, y d) se refiere a la competencia y las capacidades para ejercer sus funciones.[39]

8. Colisión con otros derechos

La vida privada no es un derecho absoluto, puede ser limitado frente la existencia de otro bien jurídico que requiera protección, respetando, de todas formas, los márgenes constitucionales y contenidos esenciales del derecho. Por tanto, el conflicto de derechos debe plantearse en términos de ponderación o adecuación. La privacidad goza del máximo nivel normativo, por lo que no hay primacía de un cierto bien jurídico sobre otro sino de efectiva o no aplicación.

Frente a una colisión debe realizarse una "ponderación de derechos, buscando reducir al máximo los derechos en conflicto, ya que todos constituyen aspectos derivados de la dignidad de la persona humana. (…) Entre derechos fundamentales no se puede hablar de jerarquía sino de equilibrio, ya que tanto la honra, la privacidad, la libertad de opinión y de información, se encuentra en el mismo nivel de derechos protegidos".[40]

[39] Corte IDH. Caso Fontevecchia y D`Amico Vs. Argentina. Fondo, Reparaciones y Costas. Sentencia de 29 de noviembre de 2011. Serie C No. 238. [en línea] <http://corteidh.or.cr/docs/casos/articulos/seriec_238_esp.pdf> [consulta: 9 junio 2014]
[40] NOGUEIRA, Humberto. El Derecho a la Información … op cit nota Nº37. 46 p.

El principio de lesividad expresa que “el derecho a la autodeterminación contenido en la protección a la vida privada no es un derecho absoluto, de manera que los actos que causan daño a otros no se encuentran constitucionalmente protegidos, incluso si ello constituye un elemento central de la identidad personal.”[41]

La difusión de un hecho de la vida privada, aun cuando pueda producir una turbación moral o espiritual, puede ser objeto del derecho a informar cuando el hecho descrito interese a la sociedad toda. Frente a esta colisión de derechos, la doctrina mayoritaria estima que debe primar el derecho a la información, pues se ve involucrado un interés público que tiene mayor jerarquía que el privado. Este examen de cuestiones debe ser juzgada por un tribunal.

9. Responsabilidad

Debe tenerse en consideración que no existe problemática alguna si lo que se divulga es de contenido público accesible a todas las personas, “una vez dada una información, saliéndonos incluso del ámbito de la privacidad, se transforma en un bien público, y otros periodistas u otros medios de difusión

[41] QUEZADA Rodríguez, Flavio. 2012. La protección de Datos Personales en la Jurisprudencia del TC. Vol. 1 Nº 1. Chile. Revista Chilena de Derecho y Tecnología. 136 p.

pueden divulgarla con la sola reserva de dar noticia de su fuente."[42] La dificultad recae cuando se da a conocer un aspecto de su vida privada que no se quiere mostrar.

La afectación ante la difusión de un hecho de la vida de la persona, debe considerar un prototipo de persona media sin considerar el sujeto real a quien afectó la difusión. "Constituye un ataque no justificado al derecho a la privacidad la difusión de hechos que causen turbación moral a una persona normal, considerándose como tal a un individuo medio o utilizando las figuras del Código Civil, a un 'buen padre de familia'"[43]

La veracidad de una información no implica que no exista responsabilidad. El agravio que se produce es de la esencia del derecho. Es decir, aun cuando se haya empleado la diligencia necesaria para obtener alguna información y ella sea verdadera, no significa que no se responderá por su publicación si esta produce daño. E incluso la ausencia de "*animus injuriandi*" en quien difunde lo íntimo, no exime de responsabilidad. Desde el punto de vista constitucional no se requiere probar el perjuicio para alcanzar la protección: una intromisión sin consentimiento en la esfera protegida merece amparo.

[42] BARROS. 1998. Honra, privacidad. op. cit. nota Nº 13. 55 p.
[43] LYON Puelma, Alberto. Teoría de la personalidad… op cit nota Nº 30. 92 p.

En Chile, el remedio procesal general más utilizado para proteger el derecho a la privacidad es el recurso de protección[44], a pesar de la existencia del *habeas data*[45]. El artículo 19 Nº 4 de la CPR cubre "el derecho a la intimidad corporal frente a indagaciones por parte de terceros; el derecho a la propia imagen, que faculta a una persona a impedir que otro capture esa imagen o la use; el derecho al secreto o a la autodeterminación informativa."[46]

Las acciones que tiene el titular del derecho a protección de la vida privada son siempre de responsabilidad ulterior, pues no se permite un mecanismo de censura previa.

Existen acciones penales por injurias o calumnias cuando se incida lesivamente sobre la vida privada y el honor, pero debe tenerse en consideración que la protección del derecho a la intimidad decae si media el consentimiento del interesado o interés público involucrado.

Todos los países que han dictados leyes de protección de datos, con la excepción de la Privacy Act de 1974 de E.E.U.U., han creado órganos y/o autoridades de control encargados de la aplicación de la ley. "Esta experiencia

[44] Entre noviembre del año 2013 y abril del año 2014 se han presentado más de 40 recursos de protección ante la Corte Suprema de nuestro país según investigación de la propia autora de esta tesis.
[45] ALDUNATE Lizana, Eduardo. 2007. Panorama actual del amparo y hábeas corpus en Chile. Chile. Estudios Constitucionales, Año 5 N° 1, ISSN 0718-0195, Universidad de Talca. 27 p.
[46] PEÑA González, Carlos. Informe sobre el proyecto de ley de protección del honor y la intimidad de las personas. 85 p.

en el derecho comparado el legislador chileno la conoció, como consta de las actas legislativas, pero no tuvo la voluntad ni la decisión de aplicarla".[47]

"(…) La obtención de un nivel de protección adecuado para los derechos fundamentales de las personas concernidas por el tratamiento de datos supone, imprescindiblemente, incorporar en nuestra normativa una autoridad de control especialmente avocada a velar por el cumplimiento de la misma."[48]

Actualmente la información personal de los chilenos circula libremente y legalmente en empresas dedicadas al tratamiento masivo de datos, transferida sin control, e incluso filtrada desde servicios públicos a entidades comerciales, sin ningún tipo de sanción[49]. Por eso es tan necesaria la dictación de legislación eficaz y actualizada, que garantice el pleno resguardo y ejercicio de los derechos.

[47] ANGUITA Ramírez, Pedro. 2007. La protección de datos personales en el derecho y la vida privada. Régimen jurídico, jurisprudencia y derecho comparado. Editorial Jurídica de Chile. p. 554

[48] Cerda Silva, Alberto. 2003. La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales. Tesis para optar al grado de Magister. Facultad de Derecho. Universidad de Chile. 237 p.

[49] Casos como la filtración de bases de datos de FONASA a la multitienda La Polar, entrega irregular de datos personales entre isapres y farmacias, y filtración de base de datos de usuarios desde el Registro Civil.

CAPITULO II. DATOS PERSONALES

El desarrollo de los medios de comunicación evidenció que el derecho a la intimidad no debía ser entendido como una expresión de exclusión del ámbito íntimo a terceros sino como una necesidad de disposición y control sobre la información personal que le compete al titular. Más aún, con las nuevas tecnologías y su capacidad de recoger, procesar y transmitir información, ha despertado preocupación frente a posibles vulneraciones a los derechos fundamentales.

"El progresivo incremento en el empleo de la informática por servicios públicos y particulares, ha permitido a estos disponer de más y mejor información, conforme a la cual adoptar las decisiones atinentes a sus ámbitos de competencia: así, por ejemplo, en unos casos se tratará de la concesión de subsidios o beneficios, en otros el propósito será prever el comportamiento del mercado ante la introducción de un nuevo bien o servicio."[50]

Es necesario determinar si la protección frente al tratamiento de datos personales "constituye una expresión de un derecho ya existente, cual es el derecho a la intimidad, o bien representa una nueva categoría de derecho, que garantiza a las personas facultades de información, acceso y control de sus

[50] CERDA Silva, Alberto. 2012. Legislación sobre Protección de las personas frente al tratamiento de datos personales. 6 p.

datos, independientemente de sí el tratamiento de tales datos constituye una lesión a la intimidad de las personas a quienes se refieren"[51]

En Estados Unidos la protección de datos personales queda circunscrita en el derecho a la privacidad dado la extensión del desarrollo jurisprudencial en dicho país[52]. "El concepto de *privacy* es un concepto amplio, abstracto y ambiguo. Esta amplitud del concepto sólo puede ser entendida bajo la idea propia del derecho norteamericano que concibe al juez como creador de derecho"[53]

En cambio en el derecho continental europeo se discute si el titular de datos personales tiene un nuevo derecho llamado "autodeterminación informativa" en la jurisprudencia alemana o "libertad informativa" en la doctrina italiana y española[54], separada del derecho fundamental a la privacidad, es decir, entendiendo el derecho a la vida privada y la protección de datos personales como derechos fundamentales autónomos y diferenciados.

[51] CERDA Silva, Alberto. 2003. La autoridad de control… op cit Nº 48. 124 p.
[52] En este sentido: FROSSINI, Vittorio. Los derechos humanos en la sociedad tecnológica. *1983.* Anuario de Derechos Humanos, número 2. pp. 101 – 115.
[53] SUAREZ Crothers, Christian. El concepto de derecho a la vida privada en el derecho anglosajón y europeo. 2000. Revista de Derecho. Vol. XI. Universidad de Talca. 114 p.
[54] En este sentido: PÉREZ-LUÑO, Antonio Enrique. "Los Derechos Humanos en la Sociedad Tecnológica", en Cuadernos y Debates, Centro de Estudios Constitucionales, Madrid, 1989, núm. 21, p. 138.

Como no existe una diferenciación legislativa en nuestro país entre protección a la vida privada y datos personales, debemos abocarnos al análisis y estudio de ambos conceptos indistintamente, ya que creemos que los problemas típicos de datos personales se desarrollan a la luz de la garantía protección a la vida privada. “El derecho a la autodeterminación informativa se construye a partir del derecho a la intimidad, tanto como este lo hizo sobre la base del derecho de propiedad.”[55]

1. Historia de la Ley 19.628

El 5 de enero del año 1993 fue presentada en el Senado una moción parlamentaria cuyo propósito era llenar un vacío manifiesto en el ordenamiento jurídico que otorgara una adecuada protección civil a la vida privada ante intromisiones ilegítimas. Se publicó en el Diario Oficial el 28 de agosto de 1999. Su tramitación fue “excesivamente larga al superar los seis años y seis meses antes de convertirse en una ley obligatoria para todos los habitantes de la República, lo cual revela las dificultades que tuvo el sistema político para consensuar un texto legal”[56].

[55] CERDA Silva, Alberto. 2012. Legislación sobre…op cit nota Nº 50. 9 p.
[56] ANGUITA Ramírez, Pedro. 2007. La protección de datos personales… op cit nota Nº 47. 234p.

La ley 19.628 aprobada en el año 1999, se denominó “Sobre Protección de la Vida Privada” no obstante contemplar solo un aspecto de ella, cual es asegurar el “derecho a la autodeterminación informativa, en lo referente al tratamiento de datos personales”.[57]

El autor de la moción expresó “la necesidad de legislar a la mayor brevedad posible acerca de la inquietud relativa a la protección de datos personales contenidos en archivos, registros, bases de datos y ficheros, materias en las cuales nuestro proyecto apenas sienta algunas directrices mínimas que requieren de un necesario complemento mediante una ley específica”[58]

La propuesta apuntaba a diseñar algunos mecanismos de protección frente a intromisiones ilegítimas de que puede ser objeto la vida privada de las personas en el país, instrumentos de compensación ante los eventuales daños morales y materiales que se produzcan con ocasión de tales injerencias ilegítimas, y la intensión de crear un Código o Estatuto Jurídico de la Privacidad.[59]

[57] CERDA Silva, Alberto. 2012. Legislación sobre…op cit nota Nº 50. 14 p.
[58] Historia de la ley. Compilaciones de textos oficiales del debate parlamentario, Ley Nº 19628, Biblioteca del Congreso Nacional, volumen 1, Santiago de Chile, 1999, 4 p.
[59] Ibídem.

En la moción parlamentaria que impulsó la ley, se dejó establecido que no era el propósito resolver las habituales querellas doctrinarias que da cuenta el derecho comparado, dejando las respuestas y soluciones a la doctrina nacional y jurisprudencia de los tribunales de justicia, a quienes corresponde delimitar las fronteras jurídicas de la institución, establecer su contenido, fundamento y naturaleza jurídica.[60]

2. Estructura

La ley 19.628 se compone de veinticuatro artículos permanentes y tres transitorios, distribuidos en siete títulos:

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

[60] Moción del Senador Eugenio Cantuarias Larrondo. Fecha 05 de enero, 1993. Cuenta en Sesión 20, Legislatura 325.

- Título Final, con un artículo único modificatorio del Código Sanitario.

Ha sido modificada seis veces: boletín Nº 2600-18, que dio origen a la ley Nº 20.152, que establece la comunicación al Boletín Comercial de los incumplimientos graves de deudas alimenticias; boletín N° 2735-05, que dio origen a la ley Nº 19.812, respecto de datos personales de carácter económico, financiero, bancario y comercial para favorecer la inserción laboral de personas desempleadas; boletín N° 3773-06, que dio origen a la ley Nº 20.285 sobre acceso a la información pública; boletín N° 4436-03, que dio origen a la ley Nº 20.463, que establece ciertas suspensiones al tratamiento de información de personas cesantes; boletín N° 6800-03, que dio origen a la ley Nº 20.521, que prohíbe la realización de predicciones o evaluaciones de riesgo comercial basada en información que no sea objetiva; y el boletín N° 7392-03, que dio origen a la ley Nº 20.575 que establece el principio de finalidad en el tratamiento de datos personales, conocida también como ley DICOM.

3. Ámbito de aplicación

El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujeta a las disposiciones de la ley 19.628, con excepción del que se efectúe en ejercicio de las libertades

de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19 N° 12 de la Constitución Política[61].

Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con la ley y para finalidades permitidas por el ordenamiento jurídico. Respetando el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce.[62]

4. Conceptos importantes

4.1. Dato personal

Los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.[63]

Dato es una unidad básica de información. Cuando dicha información es relativa a una persona determinada o susceptible de serlo, se denomina dato personal o nominativo, es decir una unidad de información sobre una persona determinada o determinable.

[61] Ley Nº 19.733 Sobre libertades de opinión e información y el ejercicio del periodismo.
[62] CHILE. Ministerio Secretaría General de la Presidencia. 1999. Ley 19.628…op cit nota Nº 23 Art. 1
[63] Ley 19.628…op cit nota Nº 23. Art. 2 f)

Determinable se refiere a que la identidad puede llegar a ser establecida por el responsable del tratamiento u otra persona, mediante medios razonablemente utilizados para identificar.

En términos amplios la ley permite afirmar que datos se refiere: “no sólo a contenidos en formato de texto, sino que comprende documentos en formato imagen y sonido, con tal que transmitan información concerniente a personas que puedan ser susceptibles de ser determinadas. Inclusive, debe calificarse como tales a los datos relativos a dirección de correo electrónico, más conocido como e-mail (…) Igualmente la ley reglamenta el tratamiento de los llamados ‘datos apreciativos’, aquellos que comprenden juicios, apreciaciones o valoraciones subjetivas que se predican de una persona.”[64]

4.2. Dato sensible

Aquellos 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.[65]

[64] CERDA Silva, Alberto. 2012. Legislación sobre…op cit nota Nº 50. 17 p.
[65] CHILE. Ministerio Secretaría General de la Presidencia. 1999. Ley 19.628…op cit nota Nº 23 Art. 2 g)

La ley ha puesto un especial cuidado en el procesamiento de estos datos sensibles debido a que su tratamiento puede provocar un grave atentado contra la vida privada de las personas. El principio rector es la prohibición de su tratamiento, la excepción es que una ley expresamente lo autorice, exista el consentimiento del titular de los datos, o sea necesario para otorgar beneficios de salud.[66]

4.3. Dato estadístico

Dato que en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.[67] Es decir, no admite ser ligado a una determinada persona, ya sea porque en su origen fue recogido en tales circunstancias, o porque mediante su tratamiento, la información resultante no puede asociarse a una persona determinada o determinable.

4.4. Titular de datos

Persona natural a la que se refieren los datos de carácter personal.[68]

[66] Es un elemento fundamental para los sistemas de salud tener acceso a cierta información de salud de sus afiliados, como los estados de salud síquicos y físicos, conductas sexuales y de vida, ya que de esa forma pueden realizar una adecuada y eficiente administración de sus recursos y una planificación de los beneficios a entregar.
[67] CHILE. Ministerio Secretaría General de la Presidencia. 1999. Ley 19.628…op cit nota Nº 23 art. 2 e)
[68] CHILE. Ministerio Secretaría General de la Presidencia. 1999. Ley 19.628…op cit nota Nº 23 art. 2 ñ)

Nuestra legislación de protección de datos personales se estructuró a partir del derecho a la intimidad, lo que explica porque el ámbito de protección envuelve sólo a las personas naturales. En la historia de la ley 19628 se estableció que "sólo se favorecerá a personas naturales no jurídicas, ya que el objeto del proyecto es precisamente resguardar la privacidad de las personas."[69] Lo que es plenamente concordante con nuestra jurisprudencia nacional al manifestar en diversos fallos que la aplicación de la ley 19.628 no es extensiva a las personas jurídicas.[70]

A pesar que la ley sólo permite que el titular de datos personales sea una persona natural, la ley 20.521 (año 2011) extendió la aplicación a las personas jurídicas al menos en lo concerniente a la proscripción de ciertas prácticas en el tratamiento de datos apreciativos.[71]

Es relevante que las instituciones, empresas y agrupaciones tengan un control sobre la información que a ellas concierne, por tanto debería extenderse el derecho de protección que la legislación prevé a las personas jurídicas.

[69] Intervención del diputado Ceroni. Disponible en la Historia de la Ley 19.628 en Biblioteca del Congreso Nacional de Chile.
[70] Recursos de Protección fallados por la Corte Suprema rol 10180-10, rol 1661-12, rol 3500-12, rol 3538-2013, rol 3816-2014, rol 6337-2014, por dar algunos ejemplos.
[71] Se incluyó en el artículo 9 de la ley 19.628 la prohibición de realizarse todo tipo de predicciones o evaluaciones de riesgo comercial que no estén basadas únicamente en información objetiva relativa a las morosidades o protestos de las personas naturales o jurídicas. Garantizándose que la infracción a la prohibición obligará a la eliminación inmediata de dicha información por parte del responsable de la base de datos y dará lugar a la indemnización de perjuicios.

4.5. Registro o banco de datos

Conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación y organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.[72]

4.6. Responsable del registro o banco de datos

Persona natural o jurídica privada, o el respectivo organismo público, a quien competen las decisiones relacionadas con el tratamiento de los datos de carácter personal.[73]

La progresiva expansión de las tecnologías y su uso por particulares hizo que la normativa de protección de datos no sólo fuera extendida al aparato estatal sino también a privados, estableciendo un efecto horizontal hacia los sujetos obligados a su protección, vinculando poderes públicos y privados.

Organismo público debe entenderse como las autoridades, órganos del Estado y organismos descritos y regulados por la Constitución Política de la

[72] Ley 19.628…op cit nota Nº 23. art. 2 m)
[73] CHILE. Ministerio Secretaría General de la Presidencia. 1999. Ley 19.628…op cit nota Nº 23. Art. 2 n)

República, y los comprendidos en el inciso segundo del artículo 1º de la Ley 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.[74]

.

4.7. Tratamiento de datos

Cualquier operación, complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.[75]

Es insuficiente extender los efectos de protección sólo a los procedimientos técnicos de carácter automatizado, por cuanto una base de datos manual, como un registro médico, igualmente puede producir un riesgo al derecho. “No es el soporte de los datos lo relevante, sino los riesgos aparejados en el tratamiento de ellos”.[76]

El propósito del legislador fue establecer un catálogo que previera el mayor número de acciones que puedan ser objeto los datos personales, y para

[74] CHILE. Ministerio Secretaría General de la Presidencia. 1999. Ley 19.628…op cit nota Nº 23. Art. 2 k)
[75] Ley 19.628, art. 2 o)
[76] CERDA Silva, Alberto. 2012. Legislación sobre…op cit nota Nº 50. 18 p.

precaver cualquier omisión utiliza la fórmula general de “utilizarlos en cualquier otra forma”.

4.8. Comunicación o transmisión de datos

Se refiere a dar a conocer de cualquier forma los datos de carácter personal a personas distintas de titular, sean determinadas o indeterminadas.[77]

4.9. Almacenamiento de datos

Conservación o custodia de datos en un registro o banco de datos.[78]

4.10. Fuentes accesibles al público

Registros o recopilaciones de datos personales, públicos o privados de acceso no restringido o reservado a los solicitantes.[79][80]

[77] Ley 19.628, art. 2 c)
[78] Ley 19.628, art. 2 a)
[79] Ley 19.628, art. 2 i)
[80] Para una análisis profundo del tema véase: ALVARADO, Francisco. Internet y las fuentes de acceso público a datos personales. 2013. Memoria para optar al título de Licenciado en Ciencias jurídicas y Sociales. Universidad de Chile.

4.11. Procedimiento de disociación de datos

Todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a una persona determinada o determinable.[81]

5. Hipótesis del tratamiento debido de datos

El tratamiento de datos personales sólo puede efectuarse si la ley 19.628 lo autoriza, otras disposiciones legales lo autorizan, o el titular consiente expresamente en ello.

5.1. Titular consiente expresamente en ello

La autorización del titular debe ser expresa, es decir, debe constar por escrito que la persona consiente en términos formales y explícitos. La persona debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público. La autorización es temporal, por tanto puede ser revocada, aunque sin efecto retroactivo, lo que también debe ser realizado por escrito.

[81] Ley 19.628, art. 2 l)

5.2. Autorización de la Ley 19.628

Se autoriza el tratamiento de datos sin el consentimiento del titular cuando la información proviene de una fuente accesible al público, tratamiento de datos por personas jurídicas privadas y el realizado por organismos públicos:

Las fuentes accesibles al público son registros o recopilaciones de datos personales públicos o privados, de acceso no restringido o reservado a los solicitantes.[82]

El tratamiento de datos personales por personas jurídicas privadas debe ser entendido para el uso exclusivo suyo, de sus asociados y de las entidades que están afiliadas, con fines estadísticos, de tarificación y otros de beneficio general de aquellos.[83]

El tratamiento de datos por organismos públicos debe ser entendido dentro de su competencia y con sujeción a las normas de la ley.[84]

[82] Ley 19.628, art. 4.
[83] Ley 19.628, art. 4 inciso final.
[84] Ley 19.628, art. 20.

5.3. Otras disposiciones legales

A modo de ejemplo podemos nombrar el artículo 33 y 62 del Código del Trabajo con respecto al libro de asistencia y remuneraciones respectivamente[85]; y el Art. 7 de la Ley 19.477[86] del Servicio de Registro Civil e Identificación, que permite celebrar convenios con otros organismos públicos y entidades privadas, con el objeto de proporcionar información contenida en los registros públicos del Servicio, con las limitaciones que la ley establece en lo que se refiere a la seguridad y confidencialidad de los datos.

6. Hipótesis de tratamiento especiales

6.1. Datos sensibles

Los datos sensibles no puede ser objeto de tratamiento, salvo que la ley expresamente lo autorice, exista consentimiento del titular, o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

[85] CERDA Silva, Alberto. 2002. Intimidad de los trabajadores y tratamiento de datos personales por empleadores. Revista chilena en derecho informático. 55p. [en línea] <http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/viewFile/10645/10921> [consulta: 19 junio 2014]

[86] Ley. 19.477, art. 7 i), Al Director Nacional le corresponderá "celebrar convenios con otros organismos públicos y entidades privadas, con el objeto de proporcionar información contenida en los registros públicos del Servicio, con las limitaciones que la ley establece en lo que se refiera a la seguridad y confidencialidad de los datos".

6.2. Obligaciones de carácter económico, financiero, bancario o comercial.

Solo se pueden comunicar los datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial cuando consten en letras de cambio o pagarés protestados, en cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa, o frente a un incumplimiento de obligaciones con entidades financieras o bancarias o casas comerciales.

En todo caso, no podrán ser tratados luego de cinco años desde que la respectiva obligación se hizo exigible[87]; tampoco cuando se trate de datos relativos a obligaciones que han sido pagadas o extinguidas por otro medio legal[88]; o cuando se trate de deudas con servicios de electricidad, agua, teléfono y gas.[89]

7. Principios relativos al tratamiento de datos personales

El tratamiento de datos personales está conformado por ciertos principios estructurales sobre los cuales descansa su entramado normativo. A continuación analizaremos los principios establecidos en la ley 19.628.

[87] Ley 19.628, art. 18.
[88] Ley 19.628, art. 18.
[89] Ley 19.628, art. 17.

7.1. Principio de libertad en el tratamiento de datos personales

Lejos de prohibir el tratamiento de datos personales, la ley consagró el principio de libertad intentando conjugar el interés de quienes requieren el procesamiento de datos con la garantía necesaria de protección a los derechos de aquellos a quienes se refiere. Es así como la Ley 19.628 asegura que "toda persona puede efectuar el tratamiento de datos personales"[90]

Sólo se condiciona su ejercicio a que el tratamiento se haga de forma concordante con la ley, con finalidades permitidas por el ordenamiento jurídico, y respetando el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que la ley les reconoce.

7.2. Principio de información y consentimiento del titular

El propósito legislativo fue conferir facultades al titular de los datos personales para poder controlar la información que le concierne. La legitimidad del tratamiento de datos está condicionado al consentimiento previo, libre e informado prestado por él mismo, sobre el propósito de almacenamiento de la información y su posible comunicación al público.

[90] Ley 19.628, art. 1.

La autorización conferida por el titular puede ser revocada aunque sin efecto retroactivo. Esta debe realizarse por escrito y no requiere de una causa justificada.

A pesar de la relevancia que reviste el consentimiento del titular de los datos, en determinadas circunstancias este resulta difícil o imposible de conseguir, o puede prescindirse de él en atención a la naturaleza de la fuente de la cual ha sido extraída la información o de los intereses individuales o sociales prevalentes. Sin embargo, la ley debió prever el establecimiento de una obligación del responsable del registro a informar al titular cuando los datos no sean entregados directamente por él.

Las excepciones al consentimiento del titular son los datos provenientes de fuentes accesibles al público, tratamiento realizado por personas jurídicas para los fines y usos exclusivos, y el tratamiento de datos realizados por organismos públicos.

7.2.1. Fuente accesible al público

Está definida en la ley como “los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los

solicitantes". Debiendo ser entendida como aquellas que por expresa disposición de la ley revista tal carácter.

Los datos pueden ser recolectados de fuentes accesibles al público prescindiendo del consentimiento del titular si[91]:

Son de carácter económico, financiero, bancario o comercial.

Se contienen en listados relativos a una categoría de personas que se limiten a indicar antecedentes de pertenencia del individuo a un grupo, como su profesión o actividad, títulos educativos, dirección, o fecha de nacimiento.

Son necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de ventas y servicios.

Esta disposición ha tenido como idea central justificar la actividad de las empresas de marketing directo, permitiendo que la información sea recibida libremente y sin limitaciones, contemplando el derecho de excluirse manifestándoselo directamente a la empresa que le envió la información.

[91] Ley 19.628, art. 1.

Requerir el consentimiento del titular significaría un entorpecimiento a su actividad.[92]

7.2.2. Tratamiento por personas jurídicas privadas

No se requiere el consentimiento del titular cuando existe un tratamiento de datos realizado por personas jurídicas privadas para su uso exclusivo, de sus asociados y afiliados, con fines estadísticos, de tarificación y otros en su beneficio.

7.2.3. Tratamiento por organismos públicos

Dicho tratamiento no necesita del consentimiento del titular y solo podrá efectuarse dentro de las materias de competencia del respectivo organismo público, con sujeción a las normas de la ley 19.628.[93]

Respecto de datos que posean los organismos públicos relativos a condenas por delito, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena. Exceptuándose los casos en que la

[92] Informe de la Comisión de Constitución, Legislación y Justicia y Reglamento del Senado, en Dss, Sesión 63ª, p. 7487
[93] Ley 19.628, art. 20.

información sea solicitada por los Tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia.[94]

Se prevé un registro de las entidades públicas que mantengan bases de datos de competencia del Servicio de Registro Civil y de Identificación[95], donde debe constar el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y la descripción del universo de personas que comprende, todo lo cual está definido en el Reglamento 779 o "Registro de Bancos de Datos Personales a cargo de Organismos Públicos"[96]

Por otro lado, la Ley 20.285 Sobre Acceso a la Información Pública, regula el principio de transparencia de la función pública, el derecho de acceso a la información de los órganos de la Administración del Estado, los procedimientos para el ejercicio del derecho y para su amparo, y las excepciones a la publicidad de la información. En su artículo 33 letra m) faculta al Consejo para la Transparencia[97] para velar por el debido cumplimiento de la ley 19.628, por parte de los órganos de la Administración del estado, y en la letra j) para velar por la debida reserva de los datos e informaciones que

[94] Ley 19.628, art. 21.
[95] REGISTRO CIVIL. [en línea] <www.registrocivil.cl/f_banco_de_datos.html> [consulta: 27 de diciembre 2012]
[96] Publicado el Diario Oficial el 11 de noviembre del 2000.
[97] Ley 20.285, art. 31. "Créase el Consejo para la Transparencia como una corporación autónoma de derecho público y patrimonio propio". Art. 32. "El Consejo para la Transparencia tiene por objeto promover la transparencia de la función pública, fiscalizar el cumplimiento de las normas sobre transparencia y publicidad de la información de los órganos de la Administración del Estado, y garantizar el derecho de acceso a la información."

conforme a la Constitución y la ley tengan el carácter de secreto y reservado. Por lo que "ambas disposiciones exigen, en consecuencia, una atenta observancia de la aplicación de los órganos públicos realicen de las disposiciones de la ley 19.628, ya sea mediante la resolución de casos particulares o la dictación de recomendaciones."[98]

Se recomienda a los órganos de la Administración que informen al titular de los datos del propósito del almacenamiento (finalidad perseguida) y su posible comunicación a terceros. "De la misma forma, se podrá informar al titular la denominación del órgano o servicio responsable del tratamiento de la base de datos y los derechos que le asisten para la protección de sus datos personales".[99]

7.3. Principio de finalidad: uso conforme al fin

Los datos personales deben utilizarse sólo para los fines para los cuales han sido recolectados, salvo que provengan de fuentes accesibles al público. Este principio tiene cabida no sólo al instante de verificarse la recogida de datos, sino que se extiende a toda operación que recaiga sobre los mismos.

---

[98] CONSEJO PARA LA TRANSPARENCIA. Compendio de normativa chilena sobre transparencia, acceso a la información y protección de datos personales. [en línea] <http://www.educatransparencia.cl/sites/default/files/compendio_de_normativa_chilena_sobre_transparencia.pdf> 172 p. [consulta: 19 junio 2014]

[99] CONSEJO PARA LA TRANSPARENCIA. Compendio de normativa chilena… op cit nota Nº 98. 181 p.

Es así como se alude a la finalidad en cuanto a las condiciones a que debe ceñirse su tratamiento[100], al contenido de la información que debe suministrarse al titular de los datos al instante de la recogida[101], a la circunstancia a que se condiciona el uso de los datos[102], al contenido del derecho de acceso e información[103], y al registro de base de datos[104].

La Ley 20.275 además de modificar la Ley 19.628, reguló el principio de finalidad en el tratamiento de datos personales de carácter económico, bancario o comercial a que se refiere el Título III de la Ley 19.628, estableciendo que la información personal de carácter financiero sólo puede ser comunicado al comercio establecido para la evaluación de riesgo comercial y para el proceso de crédito, y en ningún caso se podrá exigir en los procesos de selección personal, admisión pre-escolar, escolar o de educación superior, atención médica de urgencia o postulación a un cargo público.

7.4. Principio de calidad

La información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos. Es decir, deben representar fielmente la realidad que predican.

[100] Ley 19.628, art. 1.
[101] Ley 19.628, art. 3 y 4.
[102] Ley 19.628, art. 3, 4, 5, 20.
[103] Ley 19.628, art. 12.
[104] Ley 19.628, art. 22.

Los datos deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado. Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos. Se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de la cual no corresponda la cancelación. El responsable del banco de datos personales procederá a la eliminación, modificación o bloqueo de los datos, en su caso, sin necesidad del requerimiento del titular.

7.5. Principio de protección especial a los datos sensibles

Los datos sensibles requieren un mayor nivel de resguardo, por lo que requieren un régimen jurídico especial pues su tratamiento constituye un serio peligro de lesión para los derechos fundamentales.

Respecto de su protección se invirtió el principio de libertad disponiendo que ellos no pueden ser objeto de tratamiento, sino por excepción.

Dichas excepciones son cuando la ley autorice, cuando exista consentimiento del titular, y cuando sean datos necesarios para el otorgamiento de beneficios de salud.

La ley no garantiza una real protección de los datos sensibles diferenciada respecto de los demás datos personales, por lo que en una futura reforma, se deberá asumir tales reparos.

7.6. Principio de seguridad de los datos

El legislador, frente a los riesgos del tratamiento de datos personales especialmente por medios automatizados, suele imponer al responsable del banco de datos la adopción de medidas de seguridad de diversa índole: "físicas, referidas a la infraestructura que las resguarda; lógicas, relativas a las precauciones técnicas adoptadas (soporte, acceso, etc.); y jurídicas, o sea de índole normativo."[105] Sin embargo, no ha prestado atención alguna a medidas concretas que han de aplicarse para brindar un adecuado nivel de cuidado de los datos.

Son los Tribunales de Justicia quienes *ex post* deberán definir cuándo se han adoptado las medidas apropiadas para el cumplimiento satisfactorio de la obligación del responsable de banco de datos. Deberá tenerse en consideración el estado del desarrollo tecnológico, la naturaleza de los datos, y los riesgos que a ellos se encuentren afectos. El responsable del banco de datos deberá acreditar que adoptó medidas de protección suficientes.

[105] CERDA Silva, Alberto. 2012. Legislación sobre…op cit nota Nº 50. 15 p.

7.7. Principio de responsabilidad o deber de secreto

Los que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo.[106]

La persona natural o jurídica privada, o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.[107]

El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.[108]

[106] Ley 19.628, art. 7.
[107] Ley 19.628, art. 23.
[108] Ley 19.628, art. 11.

7.8. Garantías ante la transmisión de datos

La Ley 19.628 establece garantías frente a la transmisión de datos en general, sin embargo no prevé disposición alguna sobre la transferencia transfronteriza de datos personales por lo que nuestra normativa goza de una "eficacia reducida".[109]

El artículo 5 de la Ley 19.628 establece que el responsable del registro o banco de datos personales puede establecer un procedimiento automatizado de transmisión siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes.

Frente a un requerimiento de datos personales mediante una red electrónica, deberá dejarse constancia de: a) la individualización del requirente; b) el motivo y el propósito del requerimiento, y c) el tipo de dato que se transmite.

[109] NOGEIRA Alcalá, Humberto. 2003. Reflexiones sobre el establecimiento constitucional del hábeas data y el proyecto de ley en tramitación parlamentaria sobre la materia. Año 3 Nº1. Talca. Ius Et Praxis. Universidad de Talca. Facultad de Ciencias Jurídicas y Sociales. 284 p.

La admisibilidad del requerimiento será evaluada por el responsable del banco de datos que lo recibe, pero la responsabilidad por dicha petición será de quien la haga.

El receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión.

Lo que no aplica cuando se trata de datos personales accesibles al público en general, o cuando se transmiten datos a organizaciones internacionales en cumplimiento de tratados y convenios vigentes.

"Pese a la relevancia que reviste el consentimiento del titular de los datos personales, la Ley no lo contempla para efectos de legitimar su transmisión, ni siquiera prevé que el responsable del banco de datos o el solicitante comunique al titular la transmisión de sus datos personales, salvo un exigua indicación de 'su posible comunicación al público' como parte del contenido del derecho a ser informado." [110]

[110] CERDA Silva, Alberto. 2012. Legislación sobre…op cit nota Nº 50. 16 p.

8. Autodeterminación Informativa: derechos del titular de datos personales

Son el derecho de información y acceso, derecho de modificación o rectificación, derecho de cancelación o derecho de bloqueo.[111] La consagración de derechos para el titular de los datos personales tiene como correlato una obligación para el responsable del banco de datos.

Estos derechos son personales, irrenunciables e ilimitados. Sin embargo, la propia ley puede establecer limitaciones a su ejercicio como cuando su solicitud impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, afecten la reserva o secreto establecido en disposiciones legales o reglamentarias, la seguridad o interés de la Nación, o sean datos almacenados por mandato legal.[112]

8.1. Derecho a la información y acceso

Es el derecho que tiene todo titular para exigir del responsable del banco de datos información que le permita saber si se trata de datos de su propiedad, y de ser así cerciorarse de su exactitud y de la licitud de su tratamiento. En

[111] Ley 19.628, art. 12.
[112] Ley 19.628, art. 15.

consecuencia, no será lícito al responsable de la base de datos esgrimir imposibilidad técnica para excusarse del cumplimiento de su obligación.

Para asegurar el ejercicio de este derecho, la ley contempla la obligación de individualizarse en un registro público creado al efecto y consignar en él el fundamento jurídico de su existencia, finalidad, tipo de datos almacenados y descripción del universo de personas a que se refiere. La problemática recae en que esta obligación sólo se impone a los organismos públicos.

El derecho de información se concreta mediante el registro de las bases de datos que permite a toda persona cerciorarse de quiénes, qué y para qué procesan datos nominativos. En cambio, el derecho de acceso es un requerimiento concreto del titular ante el responsable de la base de datos, a fin de obtener de él información que le concierne y que se encuentra incorporado en ella.

8.2. Derecho de modificación o rectificación

Es el que tiene todo titular de datos para exigir la modificación de aquellos que le conciernen cuando se trate de datos erróneos, inexactos, equívocos o incompletos. Modificación se refiere a todo cambio en el contenido de los datos almacenados en registros, si estos son erróneos, inexactos,

equívocos o incompletos. El titular del dato debe acreditar la calidad del dato que reclama.

8.3. Derecho de cancelación

Es el que tiene todo titular de datos para exigir la destrucción de datos almacenados, cualquiera fuere el procedimiento empleado para ello.

Esto ocurre cuando: el tratamiento de datos carece de fundamento legal o los datos están caducos, el titular revoca la autorización que anteriormente ha proporcionado voluntariamente, y frente a comunicaciones comerciales cuando el titular haya manifestado su voluntad de ser excluido de la base de datos.[113]

Un dato carece de fundamento legal cuando los datos nunca pudieron estar en un banco de datos o cuando se trata de datos recogidos para una finalidad distinta a la que fue recabada.

Un dato es estimado caduco cuando ha perdido actualidad por disposición de la ley, cuando ha vencido el plazo o se ha cumplido la condición prevista para su vigencia, o cuando han cambiado los hechos o circunstancias que consignaron el dato.

[113] Ley 19.628, art. 12 inciso 3 y 4.

8.4. Derecho de bloqueo

Es la facultad de todo titular de datos para exigir la suspensión temporal de cualquiera de las operaciones del tratamiento de datos cuando la exactitud de los datos no pueda ser establecida o su vigencia sea dudosa y siempre que no proceda la cancelación.

Opera en subsidio de su eliminación cuando el titular revoque el consentimiento prestado para su procesamiento o no desee figurar en una base de datos empleada en comunicaciones comerciales en forma temporal.

8.5. Derecho a obtener copia

La información, modificación o eliminación será absolutamente gratuita. Más aún, existe la obligación de proporcionar a solicitud del titular de los datos, una copia del registro alterado si se han verificado modificaciones o eliminaciones de datos, siempre que hayan transcurrido a lo menos seis meses desde una consulta anterior.

9. Derechos y obligaciones del titular del registro.

El titular del registro tiene derecho a tratar los datos, siempre que lo haga de manera concordante con la ley y para las finalidades permitidas por el ordenamiento jurídico. En todo caso, deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que la ley les reconoce.[114]

Al momento de la captura o recogida de datos, debe solicitar autorización e informar al propietario de los datos acerca de la finalidad del tratamiento, los destinatarios y cualquier antecedente de interés para aquel.

El tratamiento debe ser lícito, con datos de calidad, actualizados, con un uso conforme al fin, confidencial y respetando el derecho de los titulares de los datos personales.

10. Mecanismos de control

En derecho comparado existen dos tendencias en relación con la resolución de conflictos frente al tratamiento de datos personales.[115] Algunos

[114] Ley 19.628, art. 1 inciso 2.
[115] De todas formas, todos los sistemas prevén instancias jurisdiccionales para la resolución de litigios en relación con el tratamiento de datos personales.

Estados privilegian los sistemas de autocontrol, donde el resguardo del cumplimiento de la normativa recae en los propios interesados, es decir el responsable de banco de datos y los titulares de los datos personales. Mientras que otros, prefieren una intervención más directa, efectiva y adicional del Estado.

En Estados Unidos, la normativa permite la opción de una legislación sectorial, "esto importa un rechazo a las leyes de aplicación general promovidas por la Unión Europea y antes bien se opta por generar tantas regulaciones legales como contextos ameriten su existencia, con lo cual hace frente a la especificidad que sea requerida por la naturaleza de los datos, las finalidades de su tratamiento o de la entidad titular de la base."[116]

Son los propios interesados quienes deben velar por el cumplimiento de la normativa, ya sea a través del "ejercicio de los derechos que se reconocen al titular de los datos, o bien mediante la formulación de códigos deontológicos y adopción de disposiciones reglamentarias por los órganos responsables de sistemas de registro"[117] y mediante el establecimiento de excepciones fundadas en necesidades de orden público, prescindiendo de la consagración de una

[116] CERDA Silva, Alberto. 2003. Autodeterminación informativa… op cit Nº51. 47-75 pp.
[117] CERDA Silva, Alberto. Autodeterminación informativa… op cit Nº51. 47-75 pp.

autoridad de control pública que vele por el cabal cumplimiento de la legislación.[118]

El distingo entre un modelo u otro radica en que uno postula que "la efectiva tutela frente a los riesgos de la información exige una intervención adicional del Estado, de un organismo público independiente encargado de promover e informar sobre la legislación en cuestión, fiscalizar el cumplimiento de ella y sancionar su infraestructura, o bien instar por la sanción del infractor."[119]

10. 1 Mecanismos de autocontrol

En Estados Unidos la normativa descansa en un resguardo ejercido por los propios sujetos que intervienen en él. El titular de los datos personales posee un control individual mediante el ejercicio del derecho de información, acceso y rectificación, mientras que el responsable de su tratamiento, mediante la adopción de códigos de conducta o deontológicos.

[118] El sistema de autocontrol promovido por Estados Unidos es objeto de serios cuestionamientos. Andrew Shapiro, de la Universidad de Harvard, junto con rechazar el actual estado de desarrollo de la protección de la privacidad –especialmente de los datos personales– y repudiar un enfoque mercantilista como solución, ha abogado por la creación de un organismo federal que coordine la protección de la privacidad a nivel nacional como en el extranjero, o bien, en su defecto, cuando menos encargar a alguna entidad existente todas las políticas relacionadas con la materia. SHAPIRO, Andrew,*"The control revolution"* (1999).*"El mundo en un clic",* trad. Francisco Ramos, Grijalbo. Barcelona, 2001, pp. 259 – 268, 348 – 351.

[119] CERDA Silva, Francisco. 2008. Hacia un modelo integrado de regulación y control en la protección de datos personales. Revista Derecho y Humanidades Nº 13 / 2008/ 121 -130. 123 p.

"Los códigos de conducta representan una gran ventaja, por cuando, junto con constituir un medio de adecuación de la normativa general a la especificidad de determinados contextos de tratamiento de datos, permiten hacer frente a la obsolescencia normativa. En tanto que sus principales desventajas se asocian a la legitimidad de su proceso de elaboración y la fuerza obligatoria que se le reconoce a las mismas".[120]

Nuestra ley 19.628 carece de alguna referencia acerca de los códigos de deontológicos, por lo que los métodos de autocontrol están previstos en los derechos que el propio titular tiene ante el responsable del banco de datos.

10. 2 Mecanismos de heterocontrol

Se trata de una instancia administrativa llamada "autoridad de control" que boga por el cumplimiento normativo y quien frente a una reclamación ejerce facultades fiscalizadoras y sancionatorias; y una instancia judicial que se concreta mediante el *habeas data.*

Nuestra ley omite una autoridad de control ante la vulneración de los derechos que la ley asigna al titular de datos personales, sin embargo la Ley 20.285 confirió al Consejo para la Transparencia la competencia para velar por

[120] CERDA Silva, Alberto. 2012. Legislación sobre…op cit nota Nº 50. 36 p.

el adecuado cumplimiento de la Ley 19.62, por parte de los órganos de la Administración del Estado.[121]

La acción especial para resguardar los derechos del titular conocida como *habeas data* puede revestir dos modalidades: "preventivo, cuando tiene por objeto permitir al titular de los datos personales ser informado sobre la existencia de bases de datos que contengan datos que le conciernen y acceder a los mismos, en su caso; y, el correctivo, cuando a través de él se insta porque los datos personales que le conciernen a su titular sean corregidos, modificados o cancelados cuando su tratamiento vulnere en alguna forma sus derechos".[122]

El *habeas data* tiene lugar cuando el responsable del registro de datos no se pronuncia sobre la solicitud de información, modificación, bloqueo, cancelación o eliminación de datos formulada por el requirente dentro de dos días hábiles, o bien cuando tal solicitud fuese denegada por una causa distinta de la seguridad de la Nación o interés nacional. El titular de datos debe recurrir ante el juez de letras en lo civil del domicilio del responsable, señalando la infracción cometida, los hechos que la configuran y los medios de prueba. Su

[121] Ley 20.285 Sobre acceso a la información pública. Art. 33 m).
[122] JERVIS Ortíz, Paula. Derechos del Titular de Datos y Habeas Data en la Ley 19.628. 2002. Ponencia pronunciada en el "Seminario de Datos Personales en Chile. El Nuevo Régimen Normativo, organizado por el Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de chile, entre los días 30 de septiembre y 14 de octubre de 2002. 27 p.

procedimiento es de tramitación breve y sumaria, y es independiente de otras acciones judiciales como el recurso de protección.

11. Responsabilidad

Existen dos artículos importantes que se deben considerar, el artículo 11 que establece que el responsable de los registros o bancos donde se almacenen los datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños; y el artículo 23 que indica que el responsable del tratamiento de datos, ya sea un particular o un organismo público, debe indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de datos.

Al referirse a "tratamiento debido de datos", podemos pensar que se exige culpa o negligencia en el actuar del responsable de datos, desechando la responsabilidad de tipo objetivo siguiendo las reglas de responsabilidad Civil. Sin embargo, Cerda estipula que el "sistema de responsabilidad es objetivo, prescindiendo de la concurrencia subjetiva de la culpa y dolo, bastando solamente la constatación de tratamiento indebido"[123].

[123] CERDA Silva, Alberto. Legislación sobre protección de las personas frente al tratamiento automatizado de datos personales. 39 p.

La ley 19.628 sólo contempla normas especiales de responsabilidad civil, imponiendo al responsable del registro, la obligación de indemnizar el daño patrimonial y moral ocurrido por el tratamiento indebido de datos personales. E incluso, aun cuando el responsable haya indemnizado los perjuicios causados, esto no obsta que deba eliminar, modificar o bloquear datos de acuerdo a lo requerido por el titular y ordenado por el tribunal.

La determinación de la cuantía del daño, será determinada prudencialmente por el juez, considerando las circunstancias específicas del caso y la gravedad de los hechos, tomando además todas las providencias necesarias que estime conveniente para hacer efectiva la protección de los derechos.

12. Critica a la legislación nacional

Debe existir una compatibilización entre la legitimidad del acopio, procesamiento y transmisión de la información y los derechos fundamentales.

La intromisión de la informática y las telecomunicaciones ha obligado a reformular el concepto del derecho a la privacidad como un “derecho del

individuo a decidir por sí mismo en qué medida quiere compartir con otros sus pensamientos y sentimientos, así como los hechos de su vida personal."[124]

La ley 19.628 ha sido objeto de diversas críticas al ser insuficiente y regular sólo el tratamiento de datos y no el derecho de los titulares a controlar los mismos. Este bajo estándar de protección se produjo porque fue redactada con la asesoría directa de grupos, gremios y empresas interesadas en asegurar el negocio que constituye el procesamiento de datos personales, lo que se sumó al desconocimiento de quienes la impulsaron".

En nuestro país el control de legalidad en el tratamiento de datos, se efectúa *a posteriori* por parte del titular de los datos ejerciendo la interposición de otras vías o acciones jurisdiccionales al *habeas data,* como por ejemplo "el recurso de protección, invocando como conculcados el derecho a la honra y a la vida privada, el derecho de propiedad (esto es por la conocida propietarización de los derechos), o bien, el derecho al libre desarrollo de la actividad económica"[125]

El nombre de la ley 19.628 "Sobre protección de la vida privada", es confuso y lleva a equívocos, por cuanto regula el tratamiento de datos

[124] PEREZ-LUÑO, Antonio. 1989. Los derechos humanos en la sociedad tecnológica. Número 12. Madrid. Cuadernos y debates, Centro de Estudios Constitucionales. 138 p.
[125] JERVIS Ortíz, Paula. Derechos del Titular de Datos y Habeas Data… op cit nota Nº 122. 26 p.

personales, concepto que ha adquirido una progresiva autonomía en derecho comparado y que se ha convertido en un derecho fundamental separado de la vida privada, llamado autodeterminación informativa.

La ley carece de aspectos orgánicos esenciales, como la existencia de un registro de bases de datos particulares, de un ente fiscalizador, de un procedimiento de reclamo administrativo y sanciones eficaces, transformando el *habeas data "*en una mera declaración de intenciones, ya que por vía de las excepciones y por establecer como regla general una enorme libertad en materia de procesamiento de datos personales, se permite su 'tratamiento' sin autorización de los titulares."[126]

Si bien en Chile se dispone de una ley general que "reglamenta el tratamiento automatizado y no de datos personales concernientes a personas físicas, la cual prevé derechos y obligaciones para las partes, así como una acción procesal específica, se carece de una autoridad pública que vele por el cumplimiento de la normativa. Tan sólo se ha previsto una autoridad registral con los organismos del sector público"[127]

[126] JIJENA Leiva, Renato. Actualidad de la protección… op cit Nº 10. 414 p.
[127] CERDA Silva, Francisco. Hacia un modelo integrado de regulación… op cit nota Nº 119 . 124 p.

"(…) La inexistencia de una autoridad de control que posea facultades investigativas y sancionatorias debilita fuertemente un sistema de protección de datos dejando a las normas como las establecidas por el legislador chileno en un conjunto de buenas intenciones de carácter programático, pero inaplicables en la práctica"[128]

"Los reparos en cuanto a la certificación de las tecnologías de protección de la intimidad, a la independencia del agente de control interno, a la representatividad y legalidad de los códigos deontológicos, por mencionar algunos, encuentran oportuna respuesta en la institución de una autoridad de control. Más aún, la existencia de tal autoridad no sólo resuelve tales cuestionamientos, sino que emprende cometidos que ninguno de tales mecanismos satisface: difusión, publicidad, asistencia, fiscalización y sanción. Vale decir, la implementación de una política pública coherente con un Estado democrático que promueve las condiciones que garantizan el pleno desarrollo de las personas."[129]

"Aunque el tema de los 'datos personales o nominativos procesados computacionalmente' va mucho más allá que el problema de los protestos, de la morosidad comercial y de los archivos históricos almacenados en banco de

[128] ANGUITA Ramírez, Pedro. 2007. La protección de datos personales… op cit nota Nº 47. 554 p.
[129] Cerda Silva, Alberto. 2003. La autoridad de control… op cit Nº 48. 237 p.

datos por cierto lapso de tiempo, esta es la principal connotación que se le ha dado en Chile a la Ley 19.628."[130]

Esta normativa omite a las personas jurídicas como titulares de datos siendo que igualmente son objeto del tratamiento de datos y su información es relevante siendo imprescindible entregarle herramientas para la debida protección de sus derechos.

El único ente que lleva un registro de los banco de datos es el Registro Civil pero sólo en relación a entes estatales, excluyendo de la obligación de registro a las empresas particulares, por lo que no puede entenderse como una instancia de fiscalización. No está establecido cuál es la sanción al ente que no se registre o si verdaderamente el Registro Civil puede realizar algún control efectivo si en Derecho Público sólo puede hacerse aquello que esté expresamente permitido.

"La decisión del legislador chileno de encargar al Servicio del Registro Civil e Identificación para que llevase el Registro de los Datos Personales en poder de los organismos públicos, también merece fuertes críticas. Aparte de carecer de potestades de sanción (…) podemos sostener que es un servicio

[130] JIJENA Leiva, Renato. Actualidad de la protección… op cit Nº 10. 415 p.

público dependiente del Ministerio de Justicia sin autonomía funcional y administrativa".[131]

El concepto de fuentes accesibles al público no está claramente delimitado y ha sido transformado en la regla general, lo que trae como consecuencia práctica que como los datos son legalmente públicos "cualquiera puede procesarlos y comercializarlos, validándose definitivamente el lucrativo negocio de la venta de datos personales."[132]

No se regula la transferencia internacional de datos por lo que empresas extranjeras pueden operar libremente y sin restricción alguna, mediante internet, "con la salvaguarda de que la norma chilena es territorial y no los puede alcanzar más allá del límite jurisdiccional de Chile"[133]

Diversos proyectos de ley se han presentado al Congreso con la idea de mejorar la legislación sobre privacidad y datos personales en sus distintos aspectos. Desde el año 2000 hasta junio del 2014 se han presentado setenta y ocho proyectos de ley, de los cuales sólo seis se han transformado en ley[134], quedando setenta y dos estancados o sin la debida urgencia[135].

[131] ANGUITA Ramírez, Pedro. 2007. La protección de datos personales… op cit nota Nº 47. 555 p.
[132] JIJENA Leiva, Renato. Actualidad de la protección… op cit Nº 10. 417 p.
[133] JIJENA Leiva, Renato. Actualidad de la protección… op cit Nº 10. 418 p.
[134] Se trata de los boletines números 2600-18 que dio origen a la ley N°20.152; 2735-05 que dio origen a la ley N°19.812; 3773-06 que dio origen a la ley N°20.285; 4436-03 que dio origen a la

En los dos últimos gobiernos, se presentaron dos reformas estructurales al régimen de protección de datos personales. El primero[136], pretendía conceder facultades de autoridad al Consejo para la Transparencia para la protección y control de los datos personales pero finalmente no alcanzó a ser discutido en el Congreso Nacional. El segundo[137], proponía entregarle dichas facultades al Servicio Nacional del Consumidor, y a pesar de ser ampliamente discutido en la Comisión de Economía de la Cámara, fue rechazado por ser objeto de importantes críticas.

Es necesario un compromiso real por parte del Gobierno y del Congreso para avanzar en la materia y tener una normativa adecuada y ajustada a los estándares internacionales, que garantice una real protección a los derechos fundamentales de las personas. Para ello se requiere un estudio acabado de toda la normativa nacional al respecto y de los proyectos en curso que permita sistematizar y ordenar cuál será la política pública de nuestro país, centrada en

---

ley N°20.463; 6800-03 que dio origen a la ley N°20.521 y 7392-03 que dio origen a la ley N°20.575.

[135] Boletines números 2474-07, 2771-05, 3003-19, 3066-03, 3094-19, 3095-07, 3185-19, 3312-05, 3656-18, 3796-07, 4124-18, 4143-07, 4203-07, 4429-07, 4466-03, 4482-03, 4629-07, 4959-03, 4972-03, 5009-06, 5053-07, 5122-07, 5309-03, 5320-03, 5351-07, 5356-07, 5365-07, 5754-07, 5883-07, 5999-07, 6120-07, 6298-05, 6353-07, 6495-07, 6594-07, 6598-06, 6854-03, 6914-03, 6939-03, 6979-06, 6982-03, 6994-07, 7026-07, 7055-07, 7093-03, 7132-03, 7158-05, 7232-03, 7282-07, 7715-03, 7732-07, 7776-03, 7777-07, 7794-07, 7808-13, 7831-07, 7833-13, 7864-03, 7886-03, 8086-04, 8143-03, 8175-03, 8208-07, 8222-11, 8275-07, 8559-03, 8589-07, 9242-10, 9252-15, 9388-03, 9384-07 y 9308-07. El presente índice de boletines fue preparado por Francisco Alvarado Ávalos para su tesis de grado titulada “Internet y las fuentes de acceso público a datos personales” y actualizada por la autora.

[136] Boletín Nº6120-07.

[137] Boletín Nº8143-03.

la tutela de la privacidad y el fortalecimiento de los derechos de los titulares y propietarios de los datos.

13. El dilema del consentimiento

Daniel Solove, académico norteamericano de la Escuela de Leyes de George Washington University, propone un cuestionamiento importante acerca del modelo de protección de la privacidad basado en el consentimiento sobre el cual están construidos todos los regímenes regulatorios del mundo.

"La autogestión de la privacidad se basa en el consentimiento: trata de ser neutral respecto del fondo –si determinadas formas de recopilar, usar o divulgar datos personales son buenas o malas- y se centra en si la gente autoriza determinadas prácticas respecto de su privacidad. El consentimiento legitima casi cualquier tipo de colección, uso o divulgación de datos personales".[138]

Sin embargo, esta forma de consentimiento no entrega a las personas un control significativo sobre sus datos, ya que existen severos problemas tanto cognoscitivos y estructurales que vale la pena analizar.

[138] SOLEVE, Daniel J. La autogestión de la privacidad y el dilema del consentimiento. 2013 En: REVISTA CHILENA DE DERECHO Y TECNOLOGÍA. Centro de Estudios en Derecho Informático. Universidad de Chile. Vol. 2 Num. 2 (2013) 13 p.

Dentro de los problemas cognoscitivos de mayor relevancia encontramos al individuo desinformado y la toma de decisión sesgada:

Los componentes más importantes de la autogestión de la privacidad son informar a los individuos sobre los datos que son recolectados y utilizados (notificación) y permitirles decidir si aceptan o no tal recolección y su uso (elección). La dificultad es que regularmente la mayoría de las personas no nota, lee o entiende estas notificaciones, ya sea porque son largas, difíciles de comprender, o la persona no está bien informada acerca de la materia. Por otro lado, la mayoría de las personas carecen de la pericia suficiente para sopesar las consecuencias de autorizar determinados usos o divulgaciones de sus datos, ya sea porque no sopesa adecuadamente los beneficios o riesgos, o por falta de interés.

"Obstáculos a la autogestión de la privacidad: 1) la gente no lee las políticas de privacidad; 2) si las leen, no las entienden; 3) si las leen y las entienden, usualmente carecen de los conocimientos y pericias necesarios para tomar una decisión informada; y 4) si las lee, entienden y pueden tomar una decisión informada, su decisión puede verse sesgada por varias dificultades producidas en el proceso de toma de decisiones."[139]

[139] SOLEVE, Daniel J. La autogestión de la… Op cit Nº 139. 23 p

El resultado es que las decisiones son susceptibles de problemas como racionalidad limitada, saber cómo proceder y generar soluciones, y la dificultad de conceptualizar la privacidad.

Los problemas estructurales que impiden evaluar adecuadamente los costos y beneficios del consentimiento son que hay demasiadas entidades que recolectan, utilizan y dan a conocer datos, lo que no permite poseer el tiempo suficiente o los recursos para que una persona administre su privacidad con todas ellas. Además, es difícil analizar cómo serán utilizados los datos en el futuro. “Pequeños pedacitos de información pueden decir mucho cuando son combinados”[140], e incluso pueden ayudar a realizar predicciones sobre futuros comportamientos. Por otro lado, se agrava la problemática por el hecho que las personas se inclinen por beneficios inmediatos, incluso cuando puedan existir detrimentos más adelante, pues los efectos dañinos del uso de datos pueden sólo emerger a través del tiempo.

La privacidad tiene un impacto social enorme: la innovación depende de ella a medida que se recolecta información e ideas a través de la tecnología, y tiene efectos distributivos que benefician a algunos y perjudican a otros.

[140] SOLEVE, Daniel J. La autogestión de la… Op cit Nº 139. 25 p

“La privacidad entonces, hace más que proteger a las personas individualmente consideradas. Promueve un cierto tipo de sociedad, ya que las decisiones de las personas sobre la propia privacidad afectan a toda la sociedad, y no solo a ellas.”[141]

Muchas empresas de Internet ofrecen contenidos de manera gratuita, usando el análisis o la venta de datos personales como fuente de ingreso. Si las personas se negaran a dar su consentimiento para el uso de sus datos, estos modelos de negocio fracasarían.

Cualquier solución debe confrontar este complejo dilema. Las medidas paternalistas niega la libertad para tomar decisiones voluntarias y puede entorpecer el procesamiento que no cause daño, y que incluso podría ser beneficioso. Pero un mundo sin autogestión de la privacidad sería problemático ya que las personas tienen derecho a saber cómo se utiliza su información para poder tomar decisiones acerca de sus usos, y ser beneficiado sin recibir daños.

Solove expone que no se debe abandonar el paradigma de la autogestión de la privacidad a través del consentimiento, pero tampoco se puede hacer extensiva más allá de sus límites. Para seguir avanzando:

[141] SOLEVE, Daniel J. La autogestión de la… Op cit Nº 139.14 p.

1) Se debe desarrollar un enfoque coherente del consentimiento, que dé cuenta de los conocimientos que las ciencias sociales tienen que aportar sobre cómo las personas toman decisiones acerca de sus datos personales;

2) se debe reconocer que la gente puede participar en la autogestión de su privacidad sólo en determinados casos;

3) se debe ajustar el momento en que se aplique la privacidad, centrándose en los usos posteriores; y,

4) se deben desarrollar normas de privacidad más de fondo."[142]

[142] SOLOVE, Daniel J. La autogestión de la… Op cit Nº 97. 43 p.

CAPÍTULO III. GOOGLE

La información es el poder de nuestra era y Google es el rey de los motores de búsqueda de Internet. “Para millones de internautas en todo el mundo, posiblemente para los menos expertos, Google “es internet” en sí mismo. Por eso no resulta extraño escuchar comentarios confusos como “me voy a conectar a Google”, cuando en realidad se refieren a conectarse a la red.[143]

Mediante una fórmula algorítmica descubrió el método perfecto de organizar la información mundial disponible en la web para entregarla de manera sencilla y útil, permitiendo el acceso al conocimiento de forma rápida y gratuita de forma universal.

“Nos guste o no, es la herramienta imprescindible que nos guía en el laberinto de internet: noticias, ocio, imágenes, diccionarios, libros, etc., entre mucha otra información a la que se puede acceder de manera instantánea a través de los servicios de la empresa de Mountain View.” [144]

[143] SUAREZ Sánchez-Ocaña, Alejandro. 2012. Desnudando a Google. La inquietante realidad que no quieren que conozcas. Madrid. Deusto. 26p.
[144] SUAREZ Sánchez-Ocaña, Alejandro. 2012. Desnudando a… op cit nota Nº144. 56p.

Sin embargo, hay que ser precavidos y conscientes que también es una base de datos central para obtener información de los usuarios mediante el almacenamiento proveniente de los distintos servicios que ofrece.

Todos los días millones de usuarios proporcionan a Google un acceso sin restricciones a grandes cantidades de datos personales, información que se registra y mantiene con la función de facilitar la identificación de los usuarios para diversos fines. Y el peligro está ahí, creciente entre distintos actores de la sociedad que se interesa no sólo en relacionar al usuario con publicidad específica derivada de sus propios intereses sino que también en intensiones de persecución privada o gubernamental.

El año 2011, el gobierno de Chile implementó un monitoreo de redes sociales con la finalidad de “recoger el parecer de los ciudadanos” lo que causó gran revuelo nacional al considerarse un control desproporcionado del Estado sobre los ciudadanos[145]. En Junio de 2014 se dio a conocer que la Policía de Investigaciones utilizaba datos de Facebook para atrapar delincuentes, a través de un "Empadronamiento digital".[146]

[145] ONG DERECHOS DIGITALES. Sobre el monitoreo de Internet por el Gobierno. [en línea] <https://www.derechosdigitales.org/2085/sobre-el-monitoreo-de-internet-por-el-gobierno/> [consulta: 03 julio 2014]

[146] LA SEGUNDA. Trabajo policial usa cada vez más los datos de Facebook para atrapar delincuentes. [en línea] <http://www.lasegunda.com/Noticias/Nacional/2014/06/942158/trabajo-policial-usa-cada-vez-mas-los-datos-de-facebook-para-atrapar-delincuentes> [consulta: 03 julio 2014]

Entre Julio y diciembre del año 2013, diversos organismos públicos en Chile enviaron ciento cuarenta y un solicitudes de información personal a Google y Youtube, de los cuales se entregaron ciento noventa y nueve cuentas y usuarios especificados.[147]

La filosofía de la empresa es de permanente superación, llegar cada vez más alto, más lejos y más rápido. Su adquisición de nuevos productos es insaciable.[148] Ha visualizado áreas inexploradas hasta convertirlas en herramientas útiles e imprescindibles.

[147] GOOGLE. Informe de Transparencia [en línea] <http://www.google.com/transparencyreport/userdatarequests/countries/> [consulta: 03 de julio 2014]

[148] Sólo en lo que va del primer semestre del 2014, Google ha adquirido 20 empresas, entre las que podemos encontrar: Bitspin, aplicación de reloj y alarmas para android. Nest Labs Inc, fabricante de termostatos inteligentes. Impermium, empresa especializada en ciberseguridad. DeepMind Technologies, compañía privada de inteligencia artificial. SlickLogin, empresa que crea contraseñas de audio de alta frecuencia. Spider.io, startup dedicado a detectar malware en publicidad online. GreenThrottle, fabricante de mandos de control dirigidos a los dispositivos móviles con Android. Titan Aerospace, fabricante de drones. Rangespan, 'startup' especializada en predecir los productos que demandarán los clientes en sus compras. Adometry, compañia de análisis de trafico web y campañas de marketing. Myenergy, desarrolladora de la comprensión y dirección consumo doméstico de energía. Appetas, servicio que desarrolla sitios web para restaurantes. Stackdriver, servicio de monitorización de la nube. Quest Visual, propietaria de una herramienta que permite al usuario traducir un texto impreso solo dirigiendo una cámara hacia él. Divide, Herramienta de seguridad para dipositivos android. Skybox Imaging, empresa de satélites. mDialog, empresa que ayuda a las compañías de medios a analizar y obtener beneficios de la publicidad. Alpental Technologies, startup de telecomunicaciones inalámbricas. Dropcam, firma de cámaras wifi. Appurify, startup que permite a los desarrolladores automatizar las pruebas y la optimización de sus aplicaciones móviles y sitios web. Songza, servicio de streaming musical.

La amenaza reside en que si Google dispone del conocimiento, de la información, toda la tecnología y controla el tráfico de usuarios, puede también convertirse en el único planificador y emplazador de contenido de Internet, es decir el monopolio del tráfico en la web.

La omnipotencia de Google ha generado preocupación internacional. Defensores de los Derechos Humanos, organizaciones de la sociedad civil y otros actores públicos y privados están intranquilos frente a las modificaciones de sus términos de uso:

"Google no nos pregunta si a nosotros, sus clientes, nos importaba que los datos se fusionaron y se utiliza en nuevas formas", dijo Jim Killock, director ejecutivo de la Open Rights Group, un activista digital. "La mayoría de la gente no tendrá más remedio que aguantar el cambio. Eso está mal."[149]

Frente al desconocimiento del valor de aspectos de nuestra vida privada, es interesante y a la vez necesario analizar si esta actualización se adecua a los estándares constitucionales y legales de protección de la vida privada en Chile.

[149] GOOGLE PRIVACY POLICY GETS PUBLIC AIRING. 2012 [en línea] <http://www.ft.com/cms/s/2/7d8c375c-6489-11e1-9aa1-00144feabdc0.html#axzz39jfxJA9Z> En Inglés: Google didn't ask us if we, their customers, minded our data being merged and used in new ways," said Jim Killock, executive director of the Open Rights Group, a digital activist. "Most people will have no choice but to put up with the change. That is wrong." [consulta: 12 agosto 2012]

1. Descripción general

Google INC es la empresa propietaria de la marca Google, cuyo principal producto es el motor de búsqueda de contenido en Internet, el cual mediante la utilización de diversos programas y cálculos matemáticos encuentra resultados de información acorde a los requerimientos y preferencias del usuario. “La misión de Google es organizar la información del mundo y hacerla universalmente accesible y útil”[150]

Sus fundadores Larry Page y Sergey Brin se conocieron en la Universidad de Stanford y extrajeron el nombre a partir del juego de palabras del término "gúgol", utilizado para el número uno seguido de 100 ceros, queriendo demostrar el gran alcance de rastreo de contenidos en la web.

La empresa ofrece distintos servicios para usuarios[151] entre los que podemos nombrar:

1.1. Productos de búsqueda

- Barra Google: cuadro de búsqueda en el navegador.

[150] GOOGLE. La misión de Google es organizar la información del mundo y hacerla universalmente accesible y útil. [en línea] <https://www.google.cl/intl/es/about/company/> [consulta: 12 agosto 2012]

[151] GOOGLE. Nuestros productos y servicios. [en línea] <https://www.google.cl/intl/es/about/company/products/> [consulta: 12 agosto 2012]

- Búsqueda en la web: busca contenidos en millones de páginas web.
- Herramientas de búsqueda web: funciones especiales para ayudar a encontrar exactamente lo que se busca.
- Google Chrome: navegador que ofrece rapidez, estabilidad y seguridad.
- Google Earth: información geográfica del mundo.
- Imágenes: búsqueda de imágenes en la web.
- Libros: búsqueda en el texto completo de libros.
- Google Maps: direcciones y directorio de negocios.
- Noticias: búsqueda de noticias.
- Búsqueda de blogs: búsqueda de blogs sobre temas favoritos.
- Académico: Búsqueda de documentos académicos.
- Alertas: permite recibir novedades por correo electrónico acerca de los temas que el usuario elija.

1.2. Productos para comunicar, mostrar y compartir

- Gmail: correo rápido, con menos spam y con tecnología de búsqueda de Google.
- Calendar: permite organizar agenda y compartir eventos.
- Docs: plataforma para crear proyectos en línea, compartirlos y acceder a ellos desde cualquier parte.
- Blogger: medio para expresar opiniones en línea.
- Grupos: permite la creación de listas de distribución y debate.

- Latitude: comprueba ubicación geográfica de las personas.
- Panoramio: medio para explorar y compartir fotos del mundo.
- Picasa: permite buscar, editar y compartir fotografías.
- Talk: envía mensajes instantáneos y permite llamar a contactos.
- Hangouts: conversaciones gratis en cualquier lugar y tiempo.
- Traductor: traduce texto, páginas web y archivos a más de 50 idiomas de forma instantánea.

1.3. Productos para el celular

- Mobile: accede a los productos de Google desde el teléfono móvil.
- Maps para móviles: consulta mapas, ubicaciones e indicaciones en el teléfono móvil.

La misión es hacer la búsqueda inteligente y rápida, desarrollando productos que mejoran la experiencia de los usuarios en la web, entregando contenido valioso y acorde al perfil de usuario existente en la bases de datos de Google.

2. Poder de la información

Google no sólo es una de las empresas más grandes, ambiciosas y poderosas del mundo sino que es la mayor base de datos personales jamás

creada en la historia. Sabe quiénes somos, nuestros secretos, aficiones, intereses, gustos, tendencias y relaciones personales.

La empresa es lo que es, no porque posea el mejor buscador de Internet de todos los tiempos, sino por el conocimiento que dispone de sus usuarios y del provecho que obtiene mediante esa información.[152]

"Toda nuestra información está lista para ser utilizada con dos fines distintos aunque complementarios. Primero, afianzar el dominio de la empresa como mayor fuente de información del mundo que se retroalimenta para conocer aún más cosas sobre ti. Segundo, y de forma evidente, explotar esa información para obtener beneficios."[153]

Google nos sigue y almacena información sobre nosotros con ayuda de las *cookies*.[154] En Google Chrome todas las cookies están permitidas de forma predeterminada[155] y es lo que permite tener un completo historial sobre nuestra actividad online.

---

[152] MASTER PLAN THE MOVIE [en línea] <http://masterplanthemovie.com/> [consulta: 10 diciembre 2013]

[153] SUAREZ Sánchez-Ocaña, Alejandro. 2012. Desnudando a… op cit nota Nº144. 34p.

[154] Las c*ookies* son pequeños fragmentos de información enviadas por un sitio web y almacenadas en el navegador del usuario. Ellas permiten llevar el control mediante el recordatorio de contraseña en determinadas páginas del servidor y además consiguen información sobre los hábitos de navegación.

[155] GOOGLE. Cómo administrar cookies y datos de sitios. [en línea] <http://support.google.com/chrome/bin/answer.py?hl=es&answer=95647> [consulta: 12 enero 2013]

Desde el momento en que nos conectamos, dejamos un rastro de datos susceptible de ser utilizado, en mayor o menor medida, por terceros. La información es atractiva no solo para Google sino para anunciantes, hackers, crackers, estafadores y gobiernos, por lo que la seguridad de ella debe ser primordial y garantizada.

Google recibe frecuentemente solicitudes de organismos gubernamentales y de tribunales de todo el mundo para que brinde información de los usuarios. De todas ellas, el porcentaje de solicitudes que generaron datos son, de julio a diciembre del 2013[156]:

[156] GOOGLE. Informe de transparencia. Solicitudes de información acerca de nuestros usuarios. [en línea] <http://www.google.com/transparencyreport/userdatarequests> [consulta: 3 abril 2014]

▲ País	Solicitudes de datos del usuario	Porcentaje de solicitudes para las que se generaron datos	Cuentas y usuarios especificados
Alemania	2.660	40%	3.255
Argentina	123	51%	264
Australia	780	70%	944
Austria	23	26%	114
Bélgica	162	73%	206
Brasil	1.085	49%	1.471
Bulgaria	1	0%	3
Canadá	52	25%	75
Chile	141	45%	199
China	1	0%	5
Ciudad del Vaticano	1	0%	1
Colombia	14	0%	17
Corea del Sur	353	31%	619
Costa de Marfil	2	0%	2
Costa Rica	1	0%	1
Croacia	3	0%	6
Dinamarca	58	62%	65
Ecuador	3	0%	4
Emiratos Árabes Unidos	2	0%	2
Eslovaquia	34	15%	37
Eslovenia	1	0%	1
España	545	53%	761
Estados Unidos	10.574	83%	18.254

Estonia	2	50%	4
Finlandia	13	92%	48
Francia	2.750	51%	3.378
Georgia	2	0%	4
Grecia	13	15%	29
Hong Kong	347	37%	356
Hungría	42	0%	42
India	2.513	66%	4.401
Irlanda	15	27%	51
Israel	43	65%	68
Italia	896	42%	1.084
Japón	111	60%	134
Kenia	8	63%	11
Líbano	3	0%	4
Liechtenstein	1	0%	1
Lituania	11	64%	18
Macao	3	0%	5
Malasia	2	0%	2
Malta	54	83%	60
Mauricio	1	0%	1
México	81	64%	120
Nigeria	2	0%	2
Noruega	37	73%	51
Nueva Zelanda	14	57%	17
Países Bajos	53	75%	63
Pakistán	3	0%	3
Perú	2	0%	4
Polonia	502	23%	740
Portugal	283	45%	347
Reino Unido	1.397	69%	3.142
República Checa	74	39%	88
Rumania	16	56%	33
Rusia	90	3%	202
Singapur	755	68%	847
Sudáfrica	2	0%	2
Suecia	18	28%	19
Suiza	111	67%	174

En mayo de 2011: “Google reconoció un grave fallo de seguridad que podría haber permitido a cientos hackers acceder al teléfono de cualquier individuo, ver y gestionar su libreta de direcciones o incluso saber dónde se encuentra en cada momento por medio de su calendario. Se han tomado medidas para resolverlo, pero esta falla afectó al 99,7% de los teléfonos Android en el mundo.”[157]

En abril de 2014 se dio a conocer una falla en la tecnología de encriptación web open SSL, llamada “Heartbleed”[158] que dejó expuestos datos confidenciales y sensibles de los usuarios por al menos dos años, dejando la vía libre a hackers al traspasar la codificación sin dejar huella y accediendo a datos protegidos.

“Obama estableció en enero de este año que los problemas de Internet no debían ser explotados por la Agencia de Seguridad Nacional (NSA). Pero señaló una excepción tan amplia como polémica: los espías estadounidenses podrán indagar en los fallos informáticos para prevenir un delito o proteger la seguridad nacional”[159]

[157] SUAREZ Sánchez-Ocaña, Alejandro. 2012. Desnudando a… op cit nota Nº144. 67p
[158] HEATHBLEED. Heathbleed bug. [en línea] <http://heartbleed.com/> [consulta: 03 julio 2014]
[159] EL MUNDO. Obama autorizó a la NSA a aprovechar 'agujeros' en Internet para proteger la seguridad nacional 2014. [en línea] <http://www.elmundo.es/internacional/2014/04/13/534ac004268e3ec46d8b4572.html> [consulta: 15 de abril del 2014]

Frente a la noticia que la NSA ha estado aprovechando los cables de fibra óptica de empresas de alta tecnología para interceptar fácilmente los datos que viajan sin cifrar[160], Google ha anunciado que está haciendo todo lo posible para poner a raya los ojos curiosos de espías mediante el uso de la tecnología de cifrado mejorado para que Gmail preste un servicio de correo electrónico hermético.[161]

Frente a este escenario, ¿cuáles son las armas legales que tenemos para protegernos si nuestros datos son cedidos a terceros, o peor aún, son extraídos de accesos no autorizados? En estos momentos son muy pocos los caminos realmente efectivos.

"Desde que la información personal denota valores personales, la prevención frente a su tratamiento no suscita tan solo problemas individuales, sino conflictos que importan a la sociedad en su conjunto, ya que el uso de la información permite coartar y controlar el comportamiento ciudadano".[162]

[160]RT QUESTION MORE. Google's Eric Schmidt: NSA spying 'outrageous' 2014. [en línea] <http://rt.com/usa/google-schmidt-nsa-outrageous-195/> [consulta: 15 de abril del 2014]
[161]RT QUESTION MORE. Google encrypts Gmail to safeguard against NSA snooping. 2014. [en línea] <http://rt.com/news/google-gmail-encryption-nsa-297> [consulta: 15 de abril del 2014]
[162] CERDA Silva, Alberto. 2012. Legislación sobre…op cit nota Nº 50. 7 p.

3. Principales productos y posible afectación privacidad

El número de consumidores ya no es la clave sino la información específica que de ellos se pueda recolectar. Para lograrlo Google ofrece atractivos productos de utilización gratuita que tratan datos personales y los almacenan en un perfil de usuario creado al efecto.

El juego de cruzar datos personales entre los distintos servicios persigue el fin de entregar publicidad efectiva a la medida de cada internauta y mejorar su experiencia en Internet.

3.1. Buscador Google

La globalización y nuevas tecnologías han permitido que la búsqueda de información deje de estar limitada a las bibliotecas para ahora llevarse a cabo mediante internet. Hoy en día existen múltiples de sitios web en todo el mundo de diversos creadores y contenidos.

“Los buscadores en Internet son programas o aplicaciones que residen en un sitio o página web, los cuales, al ingresar palabras en sus recuadros de búsqueda, operan dentro de la base de datos del mismo buscador y recopilan

todas las páginas que contengan información relevante y relacionada con lo que se busca."[163]

El principal desafío que enfrentan las compañías que brindan buscadores es ser capaces de brindar un orden al verdadero océano de información que es la web.

La misión de Google es organizar la información y lograr que sea útil y accesible para todos. Para ello, utiliza robots denominados comúnmente como motores de búsqueda que "son programas que escudriñan la web siguiendo los links o enlaces que van encontrando en las diferentes páginas, de tal manera de ir descubriendo y archivando lo que encuentran a su paso. Estas arañas no descansan nunca, descubriendo cada vez nuevas páginas en la red. El orden de los resultados de búsqueda en las páginas de resultados de Google se basa, en parte, en un rango de prioridad llamado *PageRank*[164].

En el método *PageRank*, las páginas web se evalúan y ponderan teniendo en cuenta los enlaces: cuantos más *links* remitan a un sitio más importante será. Pero no sólo se valoran los enlaces, sino también las páginas de las que proceden dichos enlaces. Cuanto más relevantes sean las páginas

[163] MIS RESPUESTAS. ¿Qué son los buscadores en Internet? [en línea] <http://www.misrespuestas.com/que-son-los-buscadores-en-internet.html> [consulta: 8 enero 2012]

[164] Algoritmos utilizados para asignar de forma numérica la relevancia de los documentos (o páginas web) indexados por un motor de búsqueda.

de procedencia, más valiosos serán los enlaces y, por consiguiente, la página subirá en la jerarquía.

La información que recopilan estos robots es almacenada en una gran base de datos que es consultada cada vez que se realiza una búsqueda mediante palabras clave. Esta información es ordenada y clasificada para poder entregar resultados relevantes y útiles al usuario, quedando registrada en el perfil.

El conocimiento sobre el usuario vale su peso en oro. El motor sabe qué ha buscado el internauta en el pasado y guarda esta información, ofreciéndole mejores resultados que a un desconocido.

Google guarda información fundamental sobre las búsquedas para mejorar la respuesta, mantener la seguridad de los usuarios y evitar los intentos de engaño en las búsquedas con Google. Los datos almacenados contienen la dirección IP del ordenador desde el que se ha realizado la búsqueda, el dominio Google desde el que se ha iniciado la búsqueda (.com, .de, .es, etc.), el día y la hora de la consulta, el concepto introducido (una o varias palabras) y determinada información técnica sobre el navegador (Explorer, Firefox, Safari, etc.) Además, el buscador también reconoce el sistema operativo del ordenador

y el número de identificación de la *cookie* con la que Google detecta si el usuario ya ha estado allí antes.

"Google no sólo domina el mercado de las búsquedas y la publicidad en la Red. También transforma la sociedad. Esta empresa influye en la obtención de información, afecta al aprendizaje, fomenta la cultura del «copia y pega» y actúa como el mayor registrador de datos que el mundo ha conocido. Google se ha convertido en un «gran hermano» cuya mirada pronto llegará hasta los lugares más recónditos de nuestra vida privada."[165]

Marketagent.com, citado por Reischl, se planteó la siguiente pregunta: ¿Qué buscadores conoce, al menos por su nombre? Cite espontáneamente todos los que le vengan a la memoria. El 81,8% de los encuestados nombraron a Google en primer lugar y sólo el 4,8 puso a Yahoo! a la cabeza. Lycos, con un 1,3%, ocupó el tercer puesto. ¿Dónde están AltaVista y MSN? El primero obtuvo la quinta plaza con un 0,6% y MSN se conformó con la sexta posición (0,2%), por delante todavía de AOL.[166]

[165] REISCHL, Gerald. 2008. El engaño Google. Una potencia mundial incontrolada en Internet. Primera Edición. España. Medialive Content, S.L. 30 p.
[166] REISCHL, Gerald. 2008. El engaño Google… op cit nota Nº 166. 29 p.

3.2. *Google Chrome*

Navegador sencillo y gratuito de Google que permite ejecutar aplicaciones y sitios web de forma muy rápida.

Las condiciones del servicio de Google Chrome disponible al momento de descargar el navegador[167] es un documento largo, árido, de difícil lectura dada su extensión, ignorado por el usuario, que establece ítems inquietantes. A saber:

- Reconoce y acepta que el contenido y la naturaleza de los Servicios que proporciona Google pueden variar según se considere oportuno y sin previo aviso.

- Como parte de su permanente innovación, reconoce y acepta que en cualquier momento pueda suspender, ya sea de forma permanente o temporal los servicios, o alguna de las funciones incluidas en los mismos, a su discreción y sin previo aviso.

[167] CHROME. Obtén un navegador web gratuito y veloz. [en línea] <https://www.google.com/intl/es-419/chrome/browser/?hl=es-419&brand=CHMI> [consulta: 8 enero 2012]

- Si Google inhabilita el acceso a una cuenta, es posible que la persona no pueda acceder a los servicios, a la información de su cuenta o a los archivos u otro contenido de la misma.

- Se reserva el derecho, aunque ello no constituye una obligación, de seleccionar anticipadamente, revisar, marcar, filtrar, modificar, rechazar o eliminar, parcial o íntegramente el contenido disponible.

- Podrá resolver el acuerdo legal establecido con el usuario en cualquier momento si: ha incumplido alguna de las disposiciones de las condiciones o actuó de algún modo que demuestre que no tiene intención de cumplir con tales disposiciones o que no puede cumplirlas; así se lo exige a Google la ley, por ejemplo, en caso de que la prestación de los servicios sea ilegal; el socio que se los ofrece suspendió su relación con Google o dejó de proporcionárselos; se encuentra en trámites de interrumpir la prestación de los servicios a los usuarios del país de residencia o en el que éste lo utiliza, o la prestación dejó de ser comercialmente viable..

- Algunos de los servicios se financian a través de los ingresos obtenidos de la publicidad y pueden mostrar anuncios y promociones. Podrá estar orientada al contenido de la información almacenada, a las consultas realizadas a través de estos o a otro tipo de información.

- Como contraprestación del acceso y el uso, el usuario acepta que Google muestre dicha publicidad en los servicios.

- La manera el modo y el alcance de dicha publicidad está sujeto a cambios sin previo aviso.

- Las condiciones de servicio y la relación surgida entre el usuario y Google se regirán por las leyes del Estado de California, sin contemplarse en sus normas respecto a conflicto con las disposiciones legales. El usuario y Google aceptan someterse a la jurisdicción exclusiva de los tribunales del Condado de Santa Clara (California) para resolver cualquier asunto legal derivado de las condiciones. Sin perjuicio de lo dispuesto, acepta que Google podrá reclamar por desagravio provisional, o un tipo de desagravio legal urgente que sea equivalente, en cualquier jurisdicción.

El Aviso de privacidad de Google Chrome fue modificado el 18 de octubre de 2012 y describe las prácticas de privacidad específicas de la familia de productos de Chrome, incluidos el navegador Chrome, Google Chrome Frame, el IOS Chrome y la función de navegación segura:

Cuando se utiliza cualquier navegador, para establecer conexión con los servidores, Google recibe de forma predeterminada información de registro estándar, incluida la dirección IP del sistema y una o varias cookies.

Algunas funciones de Chrome pueden enviar determinada información adicional a Google si es elegido como motor de búsqueda. De esta forma Chrome establecerá conexión con Google cuando se inicie o cuando se cambie de red para determinar la dirección web local más adecuada para el envío de las consultas de búsqueda. Al escribir una URL o una consulta en la barra de direcciones de Chrome (cuadro multifunción), las letras que se ingresen pueden enviarse al motor de búsqueda predeterminado para que la función de predicción del motor de búsqueda pueda recomendar de forma automática términos o URL que se pueda estar buscando. Si se acepta una URL o una consulta sugerida, Chrome también puede enviar esa información del navegador al motor de búsqueda predeterminado.

Al acceder al navegador de Chrome o al sistema operativo de Chrome con la cuenta de Google, se habilitará la función de sincronización. Se almacenará cierta información, como los marcadores, el historial y otras configuraciones en los servidores de Google asociados a la cuenta de Google. La información almacenada está protegida por la política de privacidad de Google. Así mismo ocurrirá si se utiliza la función de traducción, de corrección ortográfica, de entrada de voz de Chrome.

.

Si se utiliza la función de ubicación de Chrome, se enviará información de la red local a los servicios de ubicación de Google para obtener una punto territorial aproximado. Según las funciones del dispositivo, la información puede incluir datos sobre los routers Wi-Fi más cercanos, sobre la identificación móvil de las torres de telefonía más próximas, sobre la intensidad de la señal para celulares o Wi-Fi y sobre la dirección IP asignada actualmente al dispositivo.

Los sitios a los que se accede a través de Chrome reciben automáticamente información de registro similar a la que recibe Google. Estos sitios también pueden establecer sus propias cookies o almacenar datos del sitio en el sistema del usuario.

Chrome almacena localmente en el sistema del usuario algunos datos, entre los que se incluyen: información básica del historial de navegación (por

ejemplo, las URL de las páginas visitadas, un archivo de *caché* con el texto y las imágenes de esas páginas y una lista de algunas direcciones IP vinculadas desde las páginas visitadas); un índice habilitado para búsquedas con la mayoría de las páginas web a las que se ha accedido, excepto las páginas seguras que incluyen "https" en la dirección, como las de algunas entidades bancarias; capturas de pantalla en miniatura de las páginas más visitadas; *cookies* o los datos de almacenamiento de los sitios web que se visita; datos almacenados de manera local, guardados por complementos; registro de las descargas realizadas desde sitios web; identificador de dispositivo único generado por el sistema operativo de Chrome, que puede ser necesario para acceder al contenido de determinados servicios de terceros.

La información que Google recibe cuando se utiliza Chrome se procesa con el fin de operar y mejorar los otros servicios. La información que otros operadores del sitio web reciben está sujeta a las políticas de privacidad de dichos sitios web.

3.3. *Gmail*

Es el correo electrónico de Google. Fue creado en el año 2004 y posee innovaciones tecnológicas como bloqueo de spam, buscador de mensajes, vista de conversación, chat integrado de voz y video, acceso por dispositivo móvil,

gran espacio de almacenamiento de 15 GB, etiquetado y filtros de mensajes destacados, separación automática de correos electrónicos importantes, mayor seguridad por encriptación HTTPS[168] que garantiza la protección del correo, y además es gratuito[169].

Mediante esta herramienta también se puede acceder a otros servicios sincronizados como Google Talk, Google Calendar, Google Drive y Google +.

Su utilización ha ido en aumento posicionando su crecimiento en el primer lugar. De hecho al mes de octubre de 2012, Gmail tuvo 287,9 millones de usuarios únicos, mientras que Hotmail cayó al segundo lugar con 286,2 millones, y Yahoo! en tercer puesto al mostrar 281,7 millones de visitantes[170]

Para abrir una cuenta hay que registrarse, y esto significa proporcionar una serie de datos personales como el nombre, residencia, edad, sexo, número telefónico, etc. A su vez, estos datos se pueden combinar con la información que proporciona la dirección IP, es decir, con las búsquedas realizadas.

---

[168] La encriptación HTTPS permite que el correo electrónico viaje de forma segura entre el navegador web y los servidores de Gmail, de modo que las personas que compartan una red Wi-Fi pública no podrán leerlo con fines malintencionados. Novedades en Gmail. [en línea] <https://mail.google.com/mail/help/intl/es/about_whatsnew.html> [consulta: 8 enero 2012]

[169] GOOGLE. Las diez razones principales para utilizar Gmail [en línea] <https://mail.google.com/mail/help/intl/es/about.html> [consulta: 8 enero 2012]

[170] C-Net. Gmail edges Hotmail as world's top e-mail service. 2012. [en línea] <http://news.cnet.com/8301-1023_3-57543177-93/gmail-edges-hotmail-as-worlds-top-e-mail-service/> [consulta: 8 enero 2012]

Cada correo electrónico que se escribe y recibe es analizado por Google, lo que le permite entregar publicidad específica a cada usuario. Es decir, en Gmail aparece publicidad en función del contenido de nuestro correo electrónico. El análisis se excusa o califica de inofensivo porque, y así lo argumenta Google, todos los proveedores de Internet lo practican. La diferencia es que estas empresas lo escanean para encontrar virus, *spam* o *phishing.*

"Cuando un usuario abre un mensaje de correo electrónico, los equipos exploran el texto y, de manera instantánea, muestran información relevante asociada al texto del mismo. Al cerrar el mensaje, los anuncios dejan de visualizarse"[171]

Gmail permite el conocimiento de relaciones personales frecuentes del usuario, la ubicación, sus correos electrónicos, e incluso intereses en común. Uno de los grandes escándalos para la privacidad se produjo con el lanzamiento del servicio Google Buzz, donde la empresa decidió, sin autorización de los usuarios, acceder a sus libretas de direcciones de Gmail, exponiendo públicamente los datos personales de sus conocidos, amigos y

[171] GOOGLE. Más información sobre Gmail y la privacidad [en línea] <https://mail.google.com/mail/help/intl/es/more.html> [consulta: 8 enero 2012]

contactos profesionales. Tras un alud de denuncias, Google fue obligado a modificar el servicio y a pagar una multa de 6,5 millones de euros.[172]

La información que se decide eliminar puede permanecer en los servidores de Google archivado durante meses. La empresa se reserva el derecho de almacenar el contenido durante un tiempo, tanto en sus sistemas conectados a internet como *offline.*

3.4. *Youtube*

YouTube es un portal en la web en el cual los usuarios pueden subir y compartir vídeos. Fue creado por tres antiguos empleados de PayPal en febrero de 2005. En octubre de 2006, fue adquirido por Google Inc. a cambio de 1650 millones de dólares y ahora opera como una de sus filiales.

Se suben 48 horas de video por minuto, dando como resultado casi 8 años de contenido subido cada día, con cientos de millones de usuarios en todo el mundo. Usa un reproductor en línea basado en Adobe Flash para servir su contenido (aunque también puede ser un reproductor basado en el

[172] CYBERLAW CLINIC. Una demanda por violación de la privacidad frena la red Google Buzz de Gmail [en línea] <http://cyberlaw.ucm.es/expertos/loreto-corredoira/81> [consulta: 9 enero 2012]

estándar HTML5). Es muy popular gracias a la posibilidad de alojar vídeos personales de manera sencilla.

Gran parte de los vídeos que los usuarios publican en YouTube tienen música o imágenes con copyright, que la compañía sólo los retira si es requerido por el propietario de los derechos de autor. Al retirarse los vídeos la cuenta del usuario que los publicó es suspendida después de recibir, cuando menos, tres advertencias.

Variados países han bloqueado YouTube en el pasado, entre los que se encuentran Arabia Saudita, Bangladesh, la República Popular China, Pakistán, Tailandia y Turquía. En el Reino Unido y Alemania, se han bloqueado videos musicales para evitar problemas con las sociedades de derechos de autor.

Cada vez que accedemos a un video queda un registro sobre nuestra preferencia de búsqueda y luego nos sugiere videos similares o relacionados, quedando un registro sobre nuestros gustos e intereses que es almacenado en nuestro perfil.

Siendo el sitio de videos en línea más grande del mundo, muchos anunciantes quieren realizar campañas que alcancen al público. Los anunciantes pueden comprar anuncios en la página de inicio de YouTube,

páginas de resultados de búsqueda, e incluso dentro de los propios videos. También pueden organizar concursos y eventos patrocinados como conciertos en vivo y promociones de vacaciones.

La sofisticada tecnología de aprendizaje automático de Youtube, permite a los anunciantes disponer de herramientas poderosas e intuitivas, que les permite llegar al consumidor correcto en el momento oportuno.

"El marketing por categorías de interés permite orientar a los usuarios en función de su comportamiento previo relacionado con la reproducción de videos. Los anunciantes pueden seleccionar de una lista de categorías (p. ej., entusiasta automático, fanático de los deportes, etc.), y mostrar los anuncios a las personas que consideren que entran en esas categorías."[173]

3.5. Servicios de Publicidad

DoubleClick es una empresa de publicidad que desarrolla y ofrece servicios de anuncios en Internet. Fue una de las primeras empresas en representar a los sitios web para que ofrezcan espacios publicitarios a los vendedores. En el año 2008 fue adquirida por Google.

[173] YOUTUBE. Público y orientación en YouTube. [en línea] http://www.youtube.com/t/advertising_audience_targeting [consulta: 9 enero 2012]

Esta entidad posee "cookies de rastreo" que permite elaborar un expediente de hábitos de navegación. Al visitar un sitio web se realiza un seguimiento a través de otros sitios, se registra los artículos que lee el usuario, cada clic y gadgets. Por lo que su base de datos se añade a los perfiles de usuarios de Google.

Google Adsense es un servicio de publicidad para editores web. “Está diseñada para anunciantes y permite adquirir anuncios de coste por clic (CPC) o coste por impresión (CPM) correctamente orientados, independientemente de cuál sea su presupuesto.”[174] Los anuncios de Adwords se publican simultáneamente con los resultados de las búsquedas realizadas en Google, así como en los sitios de búsqueda y de contenido de la compañía.

Google AdWords es utilizado por Google para ofrecer publicidad patrocinada a potenciales anunciantes. Estos anuncios aparecen simultáneamente a los resultados de búsquedas y en zonas de páginas web, en forma de banners, que pueden ser imágenes, vídeos o texto. Google comparte los ingresos de este tipo de publicidad con los propietarios de las páginas web. En Adwords, esta área se denomina, Red de Display. Los anuncios son más flexibles que los anuncios de texto de la Red de Búsqueda.

[174] SUAREZ Sánchez-Ocaña, Alejandro. 2012. Desnudando a… op cit nota Nº144. 201p.

Podríamos entonces afirmar que Google dispone de Adwords y de Adsense, las herramientas de publicidad en internet más perfectas y con más penetración de mercado, unida a DoubleClick, que tiene una importante penetración en la publicidad de display o gráfica, lo que es un gran acaparamiento cercano a un monopolio de la publicidad en la web.

3.6. *Android*

Sistema operativo móvil basado en Linux que junto con aplicaciones middleware[175] está enfocado para ser utilizado en dispositivos móviles como teléfonos inteligentes, tabletas, Google TV y otros dispositivos. Es desarrollado por la Open Handset Alliance, liderada por Google.

Al momento de adquirir un teléfono celular con tecnología Android lo primero que nos solicita para poder iniciar el sistema es un correo electrónico de Gmail, y en caso que el usuario no tenga, da la posibilidad de crearse uno (no permite utilizar el correo electrónico de otra compañía). De esta manera el teléfono se sincroniza con todos los servicios de Google donde se encuentre el perfil de usuario.

[175] Middleware es un software que asiste a una aplicación para interactuar o comunicarse con otras aplicaciones, software, redes, hardware y/o sistemas operativos. Éste simplifica el trabajo de los programadores en la compleja tarea de generar las conexiones que son necesarias en los sistemas distribuidos. De esta forma se provee una solución que mejora la calidad de servicio, seguridad, envío de mensajes, directorio de servicio, etc.

Este sistema posee aplicaciones base que incluyen correo electrónico, programa de SMS, calendario, mapas, navegador, contactos y otros, que son registrados y almacenados por Google.

Hay que ser conscientes que mediante el uso de GPS[176], Android genera cookies de geoposicionamiento que pueden ser leídas y utilizadas desde una aplicación web y que todos los datos personales están en el dispositivo, por lo que genera un riesgo enorme a la privacidad.

En mayo de 2011 expertos informáticos de la Universidad de Ulm, Alemania, descubrieron un grave fallo de seguridad en Android que pudo afectar al 99% de los dispositivos. Este error en la seguridad permitía realizar ataques malintencionados a los usuarios de móviles y tabletas con este sistema. La agresión externa podría producirse en el momento en el que el usuario utiliza acceso a Internet público o abierto y permitía al atacante acceder a su agenda personal, su lista de contactos o fotografías almacenadas *online*.[177]

[176] GPS: sistema de navegación y localización mediante satélites. Sigla de *Global Positioning System*.
[177] 20 MINUTOS. Expertos informáticos detectan un fallo de seguridad en Android [en línea] <http://www.20minutos.es/noticia/1053847/0/fallo/seguridad/android/> [consulta: 10 enero 2012]

Otro problema ha sido las aplicaciones engañosas. El caso más reciente es el de Virus Shield[178], que estuvo una semana al tope de las aplicaciones pagas más populares de la tienda, pero que no hacía absolutamente nada: mostraba una cruz roja, afirmaba analizar el equipo para buscar problemas, luego un tilde verde y listo. Una estafa que denunció Android Police; Google la eliminó después de unos días. No tenía código malicioso, pero marcó los límites de lo que Google puede analizar cuando se publica una herramienta con estas características.

Debido a las constantes alertas de seguridad de Android, Google ha implementado una mejora que revisará los dispositivos de manera continua para asegurarse de que todas las aplicaciones se están comportando de manera segura, incluso después de la instalación. Esto incluye protecciones basadas en servicios como la verificación de aplicaciones, así como los elementos de seguridad propios de la plataforma Google Play.[179]

[178] LA NACIÓN. Google suma alertas para mejorar la seguridad en Android [en línea] <http://www.lanacion.com.ar/1679657-google-suma-alertas-para-mejorar-la-seguridad-en-android> [consulta: 11 de abril del 2014]

[179] GOOGLE. El blog corporativo para América latina. Ampliamos los servicios de seguridad de Google para Android [en línea] <http://googleamericalatinablog.blogspot.com/2014/04/ampliamos-los-servicios-de-seguridad-de.html> [consulta: 11 de abril del 2014]

3.7. *Google +*

Servicio de red social que permite a los usuarios organizar contactos en grupos o círculos, crear conversaciones sobre temas favoritos y compartirlos con otras personas con los mismos intereses. Al igual que en otras aplicaciones de la compañía, ofrece la integración con otros servicios como Gmail, Calendario, Docs, etc.

Permite los *Hangouts* que facilita el vídeochat de grupo (con un máximo de 10 personas). Posee funciones de mensajería instantánea para Android, iPhone y dispositivos de SMS para comunicarse a través de mensajes dentro de los círculos. Se pueden cargar instantáneamente fotos y videos en álbumes privados para compartir para dispositivos móviles Android.

Los “Intereses” es un conjunto de aplicaciones que permite identificar los temas en los que podrían estar interesados los usuarios en compartir con los demás. Posee la opción “+1” para permitir a la gente recomendar artículos.

En “Novedades”, se ven las actualizaciones de los círculos de conocidos. El cuadro de entrada permite a los usuarios ingresar una actualización de estado o utilizar iconos para subir y compartir fotos y vídeos. Pueden ser filtradas para mostrar sólo los mensajes de círculos específicos.

Controversia ha causado el hecho que al incorporarse al servicio se requiere la divulgación del nombre real y del género de forma obligatoria, decidiendo entre opciones de "masculino", "femenino" y "otros". En su lanzamiento, esta información fue compartida públicamente.

A partir de julio de 2012, Google obligó indirectamente a crear un perfil de Google+ para poder utilizar todas las características en otros sitios administrados por Google como por ej. YouTube. Evidentemente esto aceleró considerablemente la cantidad de usuarios de Google+, pero no ha aumentado el tiempo medio que cada usuario dedica a utilizar la red social. Algunos críticos consideran que le queda mucho para poder ganar a Facebook, temiéndose que vuelva a ser un error como Google Buzz.

3.8. *Street View*

Característica de Google Maps y de Google Earth, Street View que permite explorar lugares de todo el mundo mediante imágenes de 360 grados. Sólo contiene imágenes de lugares públicos, es decir, lo que se puede ver por la calle. Las imágenes no son en tiempo real, sólo muestran lo que los automóviles de Street View pudieron recopilar en su circulación por el lugar. Por el tiempo de procesamiento las imágenes que se observan son de meses o años atrás.

El primer reclamo provino de una neoyorquina quien al buscar su domicilio recientemente fotografiado vio y reconoció a través de la ventana a su gato, lo que la hizo reflexionar sobre la intrusión en su privacidad, algo que nadie, hasta ese momento, se había planteado públicamente.[180]

Tras las quejas iniciales y para evitar problemas de privacidad, Street View desarrolló una tecnología que permite difuminar automáticamente los rostros y matrículas identificables de autos, con el fin de no identificarlos. Sin embargo, el sistema automático encargado del tratamiento de las imágenes falla con frecuencia y sombrea elementos de la imagen que no debe y, al contrario, no detecta los algunos rostros de las personas o las matrículas de los autos. Por lo que podemos afirmar que no se eliminan todos los elementos que pueden herir la sensibilidad del usuario o menoscabar la intimidad del fotografiado.

Nos preguntamos ¿tiene Google derecho a fotografiar tu domicilio y ofrecerlo al público según las condiciones que ellos mismos establecen? ¿Hacer una fotografía nos hace propietarios de su contenido? ¿Qué podemos encontrar en la calle si fotografiamos el mundo entero?

[180] THE NEW YORK TIME. Google Zooms In Too Close for Some. [en línea] <http://www.nytimes.com/2007/06/01/technology/01private.html?_r=0> [consulta: 07 julio 2014]

Las cámaras de Google Street View han capturado en sus paseos por el mundo situaciones tales como asaltos en plena calle, gente en ropa interior captada por encima de los muros de su domicilio, robos, peleas, accidentes, personas en prostíbulos o con prostitutas en plena calle, escenas en playas nudistas, mujeres entrando en clínicas abortivas, desnudos tras el cristal de una ventana o personas orinando en plena calle.

En abril del año 2014, Google debió pagar en Italia una multa de un millón de euros por violar la privacidad al recolectar imágenes privadas para su servicio Street View.[181] La controversia data de 2010, cuando utilizó autos sin identificación, por lo que los transeúntes no podían saber que los estaban filmando ni quién lo estaba haciendo, lo que llevó a las autoridades italianas a solicitarle a Google que los identificara y que difundiera sus movimientos con tres días de anticipación en radios y diarios locales. Pese a que obedeció, las autoridades determinaron que debía pagar una multa por la recolección ilícita de información destinada a una amplia base de datos de particular importancia.

Un problema gravísimo se produjo cuando se descubrió de los automóviles de SreetView estaban equipados con tecnología que permitía la recopilación de datos personales como correos electrónicos, contraseñas y

[181] TELAM. Google paga una multa de un millón de euros por violar la privacidad. [en línea] <http://www.telam.com.ar/notas/201404/57994-google-paga-una-multa-de-millon-de-euros-por-violar-la-privacidad.html> [consulta: 04 de abril 2014]

direcciones MAC de equipos, a través de las redes abiertas de WIFI.[182] Recientemente, la Corte Suprema de Estados Unidos rechazó la apelación en que se le solicitaba que se pronunciara sobre la legalidad de la práctica por lo que Google será acusado de quebrantar las leyes de privacidad y protección de datos.[183]

4. Políticas de Privacidad

En marzo del 2012, Google modificó sus condiciones de servicio y políticas de privacidad. Retiró más de 60 políticas de privacidad de sus productos para sustituirlas en una sola, con el pretexto de hacerla más concisa y fácil de leer. Desde ese momento a la fecha ha habido cuatro modificaciones.

La información que a continuación se presentará, fue extraída directamente de las Políticas de Privacidad de Google, que se encuentran en su página web oficial.[184]

[182] BIT-TECH. Google admits Street View WiFi sniffing. 2014. [en línea] <http://www.bit-tech.net/news/bits/2010/05/17/google-admits-street-view-wifi-sniffing/1> [consulta: 14 enero 2012]

[183] ADSLZONE. Google será finalmente juzgada por el caso "Streetview". <http://www.adslzone.net/2014/07/02/google-sera-finalmente-juzgada-por-el-caso-streetview/> [consulta: 03 julio 2014]

[184] GOOGLE. Políticas de Privacidad de Google. [en línea] <https://www.google.cl/intl/es/policies/privacy/> [consulta: 07 de abril 2014]

4.1. Datos recogidos por Google

Google recoge datos para ofrecer un servicio más personalizado, determinando aspectos básicos como el idioma hasta aspectos complejos como qué anuncios son más útiles o qué contactos son más importantes para el usuario en la web.

Por ejemplo, si un usuario visita frecuentemente sitios web y blogs de jardinería, es posible que vea anuncios relacionados con la jardinería al navegar por Internet. Si ve vídeos sobre cocina en YouTube, es posible que se muestren más anuncios sobre cocina.

Se utiliza la dirección IP actual para determinar la ubicación aproximada y poder mostrar anuncios sobre servicios cercanos de entrega de pizzas a domicilio si el usuario busca "pizza" o los horarios del cine más próximo si busca "cine".

El sistema puede examinar automáticamente el contenido de los servicios de Google (por ejemplo, de los correos electrónicos de Gmail) para mostrar anuncios más relevantes. Por ejemplo, si se recibe muchos mensajes sobre fotografía y cámaras de fotos, es posible que a la persona le interese conocer una oferta de una tienda de cámaras de fotos. Por otra parte, si ha

indicado que estos mensajes son *spam*, es probable que no quiera ver la oferta. Este tipo de procesamiento automatizado es la forma que utilizan muchos servicios de correo electrónico para proporcionar funciones como el filtrado de *spam* y la revisión ortográfica.

Cuando se escribe una dirección en el campo “Para Cc” o “Cco” del mensaje que se esté redactando, Gmail sugerirá direcciones de la lista de contactos, proponiendo primero las direcciones que se usan con más frecuencia.

La recogida de datos se lleva a cabo mediante dos formas: la información que cada persona facilita a través de la entrega de datos personales solicitados para el registro de cuentas, y los datos que se obtienen a través de la utilización misma de los servicios.

Los datos que se obtienen de esta última forma se recogen a partir de la propia interacción del usuario con las páginas web que visita. Los datos incluyen:

- Información del dispositivo: modelo de equipo, la versión del sistema operativo, los identificadores únicos y los datos sobre la red móvil, incluyendo el número de teléfono. Asociado de esta

forma los identificadores del dispositivo o número de teléfono con la cuenta de Google.

- Datos de registro: en la utilización y consulta de contenido se almacena información en registros del servidor. Incluye datos sobre la utilización del servicio (consultas de búsqueda); datos telefónicos (número de teléfono, número de la persona que realiza la llamada, duración, enrutamiento de los mensajes SMS); dirección IP; información del dispositivo (fallos, actividad del sistema, ajustes del hardware, tipo de navegador, idioma del navegador, fecha y hora de tu solicitud y URL de referencia); y cookies, que permiten identificar el navegador o la cuenta determinada de una persona en Google.

- Datos sobre ubicación física: mediante utilización de las señales GPS enviadas por el dispositivo móvil, puntos de acceso Wi-Fi y antenas de telefonía móvil cercanas, se obtiene la ubicación geográfica exacta del usuario.

- Números exclusivos de aplicación: la información sobre la instalación se envía a Google al instalar o desinstalar servicios o a través de las actualizaciones automáticas.

- Almacenamiento local: a partir del web del navegador, incluyendo HTML 5 y memorias caché de datos de aplicaciones.

- *Cookies* e identificadores anónimos: el acceso e interacción con un servicio de Google incluye el envío de cookies o identificadores anónimos, así como cuando se interactúa con servicios que ofrecen servicios de publicidad o las funciones de Google que aparecen en otras páginas web.

4.2. Utilización de los datos recogidos

Los datos que se recogen a través de los servicios de Google se utilizan para "prestar, mantener, proteger y mejorar dichos servicios, desarrollar nuevas herramientas y velar por la protección de Google y de los usuarios".[185]

De igual forma, se utilizan para ofrecer contenidos personalizados en los resultados de búsqueda y anuncios relevantes, identificando al usuario en los diversos servicios, combinando la información personal y asemejando las diversas cuentas con un único individuo.

[185] GOOGLE. Política de privacidad… op cit nota Nº 137 [consulta: 14 enero 2012]

Podrá usar el nombre que se proporcione en el perfil de Google en todos aquellos servicios para cuya utilización sea necesario disponer de una cuenta de Google. Asimismo, podrá sustituir los nombres que se hayan asociado con anterioridad a la cuenta de Google de modo que la persona se identifique de forma coherente en todos sus servicios. Si algunos usuarios ya tienen la dirección de correo electrónico o los datos que sirvan para identificar a otro se podrá mostrar sus datos del perfil público de Google, como, por ejemplo, nombre y fotografía.

Frente al contacto con Google, se guarda un registro de la comunicación para poder resolver fácilmente cualquier incidencia que se haya producido. Se puede utilizar la dirección de correo electrónico para enviar información acerca de sus servicios, incluyendo información sobre próximos cambios o mejoras.

Utilizará los datos recogidos a través de las *cookies* y otras tecnologías como los contadores de visitas para mejorar la experiencia del usuario y la calidad general de sus servicios. Por ejemplo, al guardar las preferencias de idioma, podrá hacer que los servicios se muestren en el idioma que se prefiera. Cuando muestren anuncios personalizados, no asociará *cookies* o identificadores anónimos a datos especialmente protegidos como, por ejemplo, los relativos a raza, religión, orientación sexual o salud.

Podrá combinar la información personal de un servicio con la información de otros servicios de Google, incluida la información personal, para que el usuario pueda compartir contenido con otros que conozca. No combina los datos de las cookies de DoubleClick con datos de carácter personal, salvo consentimiento a tal efecto.

Pedirá el consentimiento antes de utilizar los datos para cualquier fin distinto de los establecidos en su política de privacidad.

4.3. Acceso a los datos personales y actualizaciones

La empresa pone a disposición del usuario los medios necesarios para actualizar o eliminar datos incorrectos, salvo que a su criterio estén obligados a conservar los datos para fines legales o legítimos relacionados con su actividad.

La empresa se reserva el derecho a no tramitar aquellas solicitudes que sean excesivamente reiteradas, que impliquen un esfuerzo técnico desproporcionado (por ejemplo, desarrollar un nuevo sistema o modificar de forma significativa una política vigente), que pongan en riesgo la privacidad de terceros o que resulten sustancialmente inviables (por ejemplo, solicitudes relativas a datos almacenados en copias de seguridad).

La posibilidad de acceder a nuestros datos personales y modificarlos se hará de forma gratuita, salvo que ello requiera un esfuerzo excesivo.

Al prestar los servicios de Google, se protege los datos procurando que no puedan ser eliminados de forma accidental o intencionada. Por este motivo, aunque se eliminen es posible que no se destruya de inmediato las copias residuales almacenadas en los servidores activos ni los datos almacenados en nuestros sistemas de seguridad.

4.4. Datos personales compartidos por el usuario

Muchos servicios permiten que se compartan datos entre usuarios. Los motores de búsqueda pueden indexar datos que se compartan de forma pública.

4.5. Datos personales compartidos por Google

En principio, no se comparte los datos personales con empresas, organizaciones o personas físicas ajenas a Google, salvo en los siguientes supuestos:

Consentimiento del propietario de los datos personales.

Administradores de dominio y terceros que presten asistencia a los usuarios de una organización tendrán acceso a los datos de la cuenta de Google (incluyendo dirección de correo electrónico y otros datos) para: visualizar datos estadísticos de la cuenta de usuario (en relación a las aplicaciones instaladas); cambiar contraseñas, suspender o cancelar el acceso a la cuenta, acceder a datos almacenados o conservarlos; obtener datos para cumplir requisitos previstos en la legislación o normativa aplicable o para atender cualquier requerimiento de un órgano administrativo o judicial; y para limitar la capacidad de eliminar o editar datos o ajustes de privacidad del usuario.

Tratamiento externo a filiales, organizaciones y terceros de confianza de Google para que lleven a cabo el tratamiento por cuenta de Google siguiendo instrucciones, de conformidad con las política de privacidad y adoptando medidas oportunas para garantizar la confidencialidad y seguridad de dichos datos.

Motivos legales que hagan considerar de buena fe que existe una necesidad razonable de acceder a los datos, utilizarlos, conservarlos o revelarlos a empresas, organizaciones o personas físicas ajenas a Google para: cumplir cualquier requisito previsto en la legislación o normativa aplicable o

atender cualquier requerimiento de un órgano administrativo o judicial; cumplir lo previsto en las condiciones de servicio vigentes, incluida la investigación de posibles infracciones; detectar o impedir cualquier fraude o incidencia técnica o de seguridad; proteger los derechos, los bienes o la seguridad de Google, de los usuarios o del público en general en la medida exigida o permitida por la legislación.

La empresa puede compartir datos consolidados y de carácter no personal con el público en general y con partners, incluyendo editores, anunciantes y sitios web relacionados, por ejemplo compartir públicamente datos para mostrar tendencias sobre la utilización general de los servicios.

Si la empresa participa en una fusión, adquisición o venta de activos, se asegurará mantener la confidencialidad de los datos personales e informará a los usuarios afectados antes de que sus datos personales sean transferidos o pasen a estar sujetos a una política de privacidad diferente.

4.6. Seguridad de los datos

Frente a la modificación, divulgación o destrucción no autorizada de los datos que se conservan o frente al acceso no autorizado a los mismos. En particular:

- Se encriptan servicios mediante el protocolo SSL[186].

- Se ofrece la posibilidad de configurar la verificación en dos pasos para acceder a las cuentas de Google, así como una función de navegación segura en Google Chrome.

- Se revisa la política en materia de recogida, almacenamiento y tratamiento de datos, incluyendo las medidas de seguridad físicas, para impedir el acceso no autorizado al sistema.

Se limita el acceso de los contratistas, agentes y empleados de Google a la información personal que deben procesar para Google, asegurándose que cumplan estrictas obligaciones de confidencialidad contractual, sujeta a las condiciones disciplinarias pertinentes o al despido si no cumplen dichas obligaciones.

[186] GOOGLE. Búsqueda SSL. [en línea] <http://support.google.com/websearch/bin/answer.py?hl=es&answer=173733> [consulta: 14 enero 2012]

4.7. Aplicación

La política de Privacidad se aplica a todos los servicios ofrecidos por Google Inc. y sus filiales, incluyendo los ofrecidos en otros sitios web (como, por ejemplo, servicios publicitarios), pero excluye aquellos que están sujetos a políticas de privacidad independientes, como los suministrados por otras empresas o personas físicas, incluyendo los productos o sitios que puedan mostrarse en los resultados de búsqueda y los sitios que puedan incluir servicios de Google o a los que se acceda a través de ellos.

No se regula las actividades de tratamiento de datos de otras empresas y organizaciones que anuncien servicios de Google y puedan emplear cookies, contadores de visitas y otras tecnologías para publicar y ofrecer anuncios relevantes[187].

4.8. Cumplimiento

En Google se verifica el cumplimiento de su política de privacidad de forma regular. Asimismo, se adhiere a diferentes códigos de autorregulación[188]. En caso de que reciba una reclamación formal por escrito, se pondrán en

[187] Publicidad relevante que no se mezclan con los resultados de las búsquedas sino que se enseña en los laterales o la parte superior de la página y siempre claramente identificados con la palabra “anuncios” o con sombras de color.

[188] GOOGLE. Marcos de autorregulación de Google. [en línea] <https://www.google.com/intl/es/policies/privacy/frameworks/> [consulta: 14 enero 2012]

contacto con la persona que la haya formulado para hacer un seguimiento de la misma.

Para resolver cualquier reclamación relacionada con la transferencia de datos de carácter personal que no haya podido solucionar directamente con el usuario, se compromete a trabajar con las autoridades reguladoras competentes, incluyendo las autoridades locales de protección de datos.

4.9. Modificaciones

Las políticas de privacidad pueden modificarse en cualquier momento, pero no se limitarán los derechos del usuario sin su expreso consentimiento.

Se publicará todas las modificaciones en la página https://www.google.com/intl/es/policies/privacy/, y, si son significativas, se efectuará una notificación más destacada (notificación por correo electrónico si la modificación afecta a determinados servicios). Además, se archivan las versiones anteriores para que el usuario pueda consultarlas.

Chrome, Chrome OS, Google Libros, Google Wallet y Fiber poseen políticas de privacidad específicas.

5. Condiciones de uso de los productos y servicios de Google

Al utilizar los productos y servicios proporcionados por Google Inc. se está aceptando de manera automática las condiciones de uso, lo que provoca un grave problema ya que el usuario generalmente no se informa directa y conscientemente de ellas. La última modificación en este sentido es de abril del 2014.

A continuación analizaremos las condiciones de uso disponibles en la página web de Google.[189]

Los servicios que se proporcionan son diversos, de modo que en ocasiones pueden aplicarse condiciones adicionales u otros requisitos (ej. mayoría de edad para ver ciertos contenidos en Youtube). Estas estarán disponibles junto con los servicios pertinentes y formarán parte del acuerdo que se establece al usarlos.

El usuario no puede interferir ni intentar acceder por otro método diferente a la interfaz y las instrucciones que se proporcionan. Si se incumplen las políticas o condiciones, o si se investiga una conducta indebida, Google puede suspender o dejar de proveer el servicio.

[189] GOOGLE. Condiciones del servicio de Google [en línea] <https://www.google.cl/intl/es-419/policies/terms/regional.html> [consulta: 09 de abril del 2014]

El uso no otorga derecho de propiedad intelectual alguno sobre los servicios o contenidos al que se acceda, y no se podrá utilizar a menos que se obtenga permiso del propietario o que esté autorizado por ley. No se permite utilizar marca o logotipo alguno, ni se puede eliminar, ocultar ni modificar ningún aviso legal mostrado.

Google proporciona una licencia personal, internacional, sin regalías, no cesible y no exclusiva para utilizar sus software. El usuario no puede copiar, modificar, distribuir, vender ni otorgar licencia de parte alguna de los servicios o software incluido, ni puede realizar ingeniería inversa o intentar extraer el código fuente de dicho software. Sin embargo, ofrece algunos softwares bajo licencia de código abierto.

Hay algunos servicios que permiten proveer contenido, y en este sentido la persona conservará los derechos de propiedad intelectual. Pero cuando los suba o envíe, otorgará a Google (y a aquellos con quienes trabaja) una licencia internacional para utilizar, alojar, almacenar, reproducir, modificar, crear obras derivadas (como traducciones o adaptaciones), comunicar, publicar, ejecutar públicamente y distribuir dicho contenido. Los derechos que otorga la licencia son para el objetivo limitado de operar, promocionar y mejorar los servicios, y para desarrollar otros nuevos; subsistiendo aun cuando se dejen de utilizar (por ejemplo, una empresa que el usuario haya agregado a Google Maps).

Por otro lado, los contenidos mostrados que no pertenecen a Google son de responsabilidad exclusiva de la entidad que lo pone a disposición. Pero si puede revisarlo para determinar su legalidad o si infringe sus políticas, y en este sentido podrá eliminar o rechazar su visualización.

Los sistemas automatizados analizan el contenido (incluidos los correos electrónicos) para ofrecer funciones de productos que sean relevantes, como resultados de búsqueda, anuncios personalizados, detección de software malicioso y *spam*. Este análisis se realiza cuando el contenido se envía, se recibe y cuando se almacena.

Es necesario crear una cuenta para utilizar los servicios y de esta forma es posible que se muestre el nombre de perfil, foto y las acciones que el usuario realiza en Google o en aplicaciones de terceros conectadas a la cuenta de Google (como los +1 que se hacen, las opiniones que escriben y los comentarios que se publican), incluida la aparición en anuncios y otros contextos comerciales.

El usuario puede dejar de utilizar los servicios y Google también puede dejar de brindárselos, o agregar o crear nuevos límites en cualquier momento. Se pueden modificar las condiciones principales y adicionales las que serán avisadas en su oportunidad pero es cargo del usuario revisar periódicamente

los cambios. Estas no se aplicarán retroactivamente y entraran en vigencia no antes de catorce días después de su publicación, sin embargo las modificaciones realizadas por razones legales o por nuevas funciones entrarán en vigencia de forma inmediata. En caso de cancelación de un servicio y siempre que a juicio de Google sea “razonablemente posible”, notificará con anticipación y le brindará al usuario la posibilidad de obtener su información y preservar el acceso a los datos de que es propietario.

Google no asume compromiso alguno respecto del contenido o las funciones de los servicios, ni acerca de la confiabilidad, disponibilidad o capacidad para satisfacer las necesidades del usuario. Proporcionan los servicios “tal como están”.

Cuando un servicio requiere o incluye software descargable puede actualizarse automáticamente en el dispositivo cuando haya una nueva versión o función disponible, predisponiéndose su configuración.

Si la ley lo permite, Google y sus proveedores y distribuidores no serán responsables por lucro cesante, pérdida de ganancias, de datos o financieras, ni por daños indirectos, especiales, emergentes, ejemplares o punitorios.

La responsabilidad total de Google y de sus proveedores y distribuidores por cualquier reclamo en virtud de las condiciones, incluida cualquier garantía implícita, estará limitada al monto abonado por el usuario para utilizar los Servicios.

En algunas jurisdicciones se prevén determinadas garantías, por ejemplo, la garantía implícita de comerciabilidad, adecuación para algún propósito y no infracción de derechos. En la medida permitida por ley, Google excluye todas las garantías.

En ningún caso Google y sus proveedores y distribuidores serán responsables por pérdidas o daños que no sean razonablemente previsibles.

Frente a presuntas infracciones a los derechos de autor, se responde a las notificaciones y se cierran las cuentas de los infractores reincidentes de acuerdo con el proceso establecido en la ley estadounidense de protección de los derechos de autor (U.S. Digital Millennium Copyright Act). Además, Google proporciona información para ayudar a que los titulares de derechos de autor administren su propiedad intelectual en línea.[190]

Si una empresa utiliza los servicios deberá indemnizar a Google y a sus afiliadas, directores, agentes y empleados de cualquier reclamo, pleito o acción

[190] GOOGLE. Como retirar contenido de Google [en línea] <https://support.google.com/legal/troubleshooter/1114905?rd=2> [consulta: 09 de abril del 2014]

relativa al uso o incumplimiento de sus condiciones, incluido cualquier costo o responsabilidad que surja de reclamos, pérdidas, daños, pleitos, fallos, costos de litigio y honorarios de abogados.

En caso de reclamos y controversias se aplicarán las leyes de California EEUU, a menos que el país haya estipulado que no se utilicen.

6. Problemáticas en la Política de Privacidad y Condiciones de Uso de los productos de Google que afectan el derecho a la privacidad.

"Leer todas las políticas y condiciones de uso y privacidad de los servicios digitales a los que se suscribe te tomaría 180 horas anuales, que equivalen a un mes en un empleo de tiempo completo.[191]

Al utilizar los servicios de Google aceptamos que use nuestros datos personales de acuerdo a su política de privacidad. Puede modificarse el nivel de visibilidad y limitar el uso compartido de la información, pero ¿cuántos usuarios están conscientes de esta posibilidad? Si la persona no sabe o no se ha percatado del valor de su privacidad, difícilmente sabe la importancia de configurarlo.

[191] Estudio 'The cost of Reading privacy policies' de la Universidad Carnegie Mellon, disponible en: EL FINANCIERO. Revisar las políticas de privacidad de redes sociales puede tomar 180 horas. [en línea]
<http://www.elfinanciero.com.mx/empresas/revisar-las-politicas-de-privacidad-de-redes-sociales-puede-tomar-180-horas.html> [consulta: 30 de mayo 2014].

En las políticas y principios que Google entrega en su página web se menciona su intención de mejorar la seguridad, proteger la privacidad y diseñar herramientas simples que permitan al usuario tomar decisiones y controlar la información personal. En este sentido ofrece la "verificación de dos pasos"[192], mecanismo que evita que la cuenta sea interceptada, reduciendo la posibilidad de robo de información personal. Al iniciar sesión en Google se debe introducir el nombre de usuario y la contraseña, pero posteriormente debes agregar directamente un código que se recibe en el teléfono mediante mensaje de texto, llamada de voz o su propia aplicación para móviles de Google ¿Cuál es el problema? Se promete mayor protección a los datos a cambio de la entrega del número de teléfono personal, lo que acrecienta la cantidad de información que mantienen en su base de datos. Cuando nos ofrecen un servicio o aplicación gratuita, nosotros no somos los beneficiarios sino que somos el producto.

En Gmail existen dos tipos de cuentas de usuario, una creada por la propia persona y otra por un administrador, que puede ser un empleador, institución, organización, etc. Esta última posibilidad permite que se puedan aplicar condiciones diferentes o adicionales a las establecidas por Google, entregando al administrador un acceso privilegiado a las cuentas de sus administrados, permitiendo que la monitoree o incluso la inhabilite, vulnerando

[192] GOOGLE. Acerca de la verificación en dos pasos. [en línea] <https://support.google.com/accounts/answer/180744?hl=es-419&rd=1> [consulta: 01 de abril 2014]

los derechos fundamentales, especialmente la inviolabilidad de las comunicaciones que está garantizado en el artículo 19 Nº 5 de la CPR.

¿Cuál es el límite de los sistemas automatizados que analizan el contenido incluyendo los correos electrónicos para ofrecer funciones de productos relevantes? Si como usuarios no nos interesan los anuncios personalizados ¿tenemos alguna opción para evitarlo? Las condiciones de uso son claras, si el usuario no las acepta deberá terminar su utilización.

En este contrato de adhesión, existe un desequilibrio en el poder negociador de las partes. Google es el oferente que dicta las clausulas y nosotros nada podemos hacer para cambiarlo. El problema es que está en juego información personal valiosa.

Google puede compartir datos consolidados y de carácter no personal con el público en general y con terceros de confianza, pero ¿cuál es la fórmula de distinción que utiliza para dirimir entre información personal sensible, de la que no es? De igual forma puede considerar de “buena fe” que existe “necesidad razonable” de acceder a los datos, pero no define expresamente cuáles son los motivos ni el criterio normativo para hacerlo.

La única fórmula que permite evitar la dudosa utilización de datos personales es tener un reconocimiento legal y normativo que permita al individuo decidir cuándo y cómo está dispuesto a permitir que sea difundida su información. Debemos saber específicamente la naturaleza, motivos y finalidad de ellos, pues solo así podremos controlarlo.

La sola comunicación a los usuarios de la transferencia de sus datos personales a otro organismo frente a una fusión, adquisición o venta, o que estarán sujetos a una política de privacidad diferente, no es suficiente. Es necesaria una nueva autorización expresa del titular.

El consentimiento al momento de aceptar una política de privacidad, o frente a la modificación de algunos de sus cláusulas debe ser una manifestación inequívoca de voluntad, efectuada de forma libre e informada, y nunca por defecto.

Como vimos previamente, la ley 19.628 otorga al titular el derecho de información o acceso, modificación, bloqueo, cancelación o eliminación de sus datos personales. El buscador Google según la sentencia del Tribunal Europeo de Justicia[193] realiza un tratamiento de datos personales. Entonces, si encuentro información sobre mi persona desactualizada o incorrecta en el

[193] Será analizado en el próximo apartado.

buscador, ¿podría modificarla o incluso eliminarla? Lamentablemente esta sentencia sólo es efectiva en países de la Unión Europea, donde los estándares normativos de protección de datos personales son mucho más altos que en nuestro país.

Es más que ilusorio pensar en hacer efectiva la protección de derechos si la normativa en Chile resulta insuficiente. Senadores del gobierno de Chile presentaron un proyecto de ley que establece el derecho al olvido en internet[194], pero antes de avanzar en ese sentido, lo primero es mejorar la ley en sí. En el entretanto la empresa adquiere una licencia de uso de todo lo que nosotros incluimos o agregamos en sus plataformas. Nuestra información deja de pertenecernos y aceptados que nuestros derechos sean limitados y escasos.

Google muchas veces muestra contenido que no le pertenece, siendo responsabilidad exclusiva de la entidad que lo haya puesto a disposición. Sin embargo, puede revisar, eliminar o negar la publicación del contenido si es ilegal, infringe sus políticas o la ley, especificando que eso no implica que revisen el contenido. Entonces ¿cómo pueden hacerlo? No existe ningún lineamiento que los permita dilucidar más que su propio criterio.

[194] Boletín 9388-03. Se agrega un inciso al artículo 13: Toda persona tiene derecho a exigir de los motores de búsqueda o sitios web la eliminación de sus datos personales. La falta de pronunciamiento sobre la solicitud del requirente o denegación de la misma por parte del responsable de dichos motores de búsqueda o sitios web, le dará derecho al titular a ejercer el recurso contemplado en el artículo 16

A petición de gobiernos, Google ha tenido que restringir el acceso a ciertos contenidos para adaptarse y cumplir con las legislaciones locales y poder operar en diversos mercados. De esta forma, no despliega la totalidad de los resultados relacionados con las búsquedas de las páginas que el motor tiene en cada país, lo que podríamos catalogar de censura.

A inicios de abril de 2009 YouTube dejó de transmitir videos en Alemania, al ser incapaz de alcanzar un acuerdo con GEMA, la mayor sociedad de derechos de autor alemana[195]. A finales de 2006 el Gobierno tailandés bloqueó el acceso al sitio como respuesta a la aparición de videos donde se insultaba al Rey de Tailandia, Bhumibol Adulyadej, considerado un crimen en ese país[196].

En ocasiones los usuarios de Internet en la República Popular China han presentado problemas para acceder a YouTube. Durante los disturbios en el Tíbet de 2008 YouTube fue bloqueada por el Gobierno.[197] En el 2010, Turquía reabrió el acceso a Youtube luego de dos años de bloqueo producto de una guerra de internautas nacionalistas griegos y turcos en los que se mofaban del

[195] EL MUNDO. YouTube deberá bloquear los vídeos musicales en Alemania. 2009 [en línea] <http://www.elmundo.es/elmundo/2009/04/02/navegante/1238656149.html> [consulta: 9 enero 2012]

[196] EMOL. Tailandia bloquea a YouTube por videos que se burlan del rey. 2007. [en línea] http://www.emol.com/noticias/tecnologia/2007/04/04/251598/tailandia-bloquea-a-youtube-por-videos-que-se-burlan-del-rey.html [consulta: 9 enero 2012]

[197] CNN. YouTube blocked in China. 2009. [en línea] <http://edition.cnn.com/2009/TECH/ptech/03/25/youtube.china/index.html> [consulta: 9 enero 2012]

fundador de la República turca, Mustaba Kemal Ataturk, lo que es considerado delito en base a una ley sobre ciberdelitos[198]. El pasado 27 de marzo, la Dirección de Telecomunicaciones de Turquía, restringió el acceso al servicio horas después de que en esa página se difundiera una conversación de ministros clave de seguridad sobre Siria, clasificada como secreta[199].

El problema está en el gran poder de censor que se le entrega a una empresa privada para decidir qué tipo de información se puede acceder y de qué modo ¿Son ellos los que deben asumir ese papel? Creemos que ese poder debe ser supervisado por organismos superiores.

Por eso y muchas otras razones es que es tan necesario que en Chile exista un organismo de protección de datos personales, mientras no exista, cualquier protección nacional que se intente será insuficiente.

"La supremacía de Google en el mercado (a pesar de la existencia de adversarios como Yahoo! o MSN es peligrosa para la sociedad. Cualquier empresa con mucho poder se convierte en una amenaza, porque los

[198] LA VOZ DE GALICIA. Turquía reabre YouTube tras más de dos años de bloqueo. 2010. [en línea] <http://www.lavozdegalicia.es/tecnologia/2010/10/31/00031288523645938566654.htm> [consulta: 9 enero 2012]
[199]NOTICIAS MVS. Permanecerá YouTube bloqueado en Turquía. 2014 [en línea] <http://www.noticiasmvs.com/#!/noticias/permanecera-youtube-bloqueado-en-turquia-330.html> [consulta: 21 de abril del 2014]

monopolios no sólo crean dependencia, sino que abren las puertas a la manipulación, ya sea de datos, información u opinión."[200]

Google cambia sus servicios constantemente. Por ello, es posible que añada, limite o elimine algunas funciones o características, o que se suspenda o cancele por completo un producto en cualquier tiempo, lo que es tremendamente peligroso para las personas que los utilizamos.

En caso de cancelación de un servicio y siempre que a juicio de Google sea "razonablemente posible", notificará con anticipación y le brindará al usuario la posibilidad de obtener su información y preservar el acceso a los datos de que es propietario. Pero ¿qué significa el criterio "razonablemente posible"? y ¿cuál es el plazo con debida anticipación? Complejo es que el gigante tecnológico tenga la absoluta libertad de cambiar y mejorar continuamente sus servicios, agregar o eliminar funcionalidades o características, y también suspender o interrumpirlo en su totalidad.

La predisposición de configuración de un servicio a actualizarse automáticamente es sumamente peligroso:

[200]REISCHL, Gerald. 2008. El engaño Google… op cit nota Nº 166. 30 p.

Investigadores de la Duke University, Penn State University e Intel Labs desarrollaron un programa de seguridad llamado TaintDroid, que usa un tipo de análisis para detectar y reportar cuando las aplicaciones envían información delicada a servidores remotos. Es así como descubrieron que algunas aplicaciones de Android enviaban información de GPS a los anunciantes sin el consentimiento o siquiera conocimiento de los usuarios:

"Según reportan, usaron este sistema para probar 30 aplicaciones gratis del Android Market seleccionadas al azar. El resultado fue que descubrieron que la mitad de ellas enviaban información privadas a servidores de anunciantes, incluyendo la ubicación del usuario y el número de teléfono. A veces incluso, se encontraron con aplicaciones que enviaban las coordenadas del dispositivo cada 30 segundos, incluso cuando no mostraban publicidades".[201]

¿Es Google responsable de los fines maliciosos de robo de información personal que utilizan estas aplicaciones? Debería, sin embargo en una clausula establece que éste no será responsable por lucro cesante, pérdida de ganancias, de datos o financieras, ni por daños indirectos, especiales, emergentes, ejemplares o punitorios; y en caso de serlo, se limitará al monto

[201] MODMYMOBILE. Las aplicaciones de Android enviarían información GPS a los anunciantes [en línea] <http://modmymobile.com/forums/552-general-android-esp/557091-las-aplicaciones-de-android-enviarian-informacion-gps-los-anunciantes.html> [consulta: 08 de abril del 2014]

abonado por el usuario para utilizar los servicios. Por lo que cabe preguntarnos ¿hay o no responsabilidad? En todo sistema legal, si se produce un daño por culpa o negligencia se debe responder. En ningún caso una cláusula contractual puede actuar como un eximente de responsabilidad. Además, ¿qué es lo que ocurre con la mayoría de los servicios gratuitos en que no existe dinero entregado por el usuario? ¿La indemnización sería inexistente?

Google lleva a cabo el tratamiento de los datos personales en sus servidores que están ubicados en distintos países del mundo, por lo que podrá llevarlo a cabo en una sucursal que no esté ubicado en el país de residencia del usuario, lo que genera un conflicto entre la ley de protección de datos personales del país origen con el lugar donde se realiza el tratamiento. No existe certeza que se tenga el conocimiento y se respeten las leyes de igual forma. Además puede transferir información con filiales, organizaciones y terceros de confianza, ¿hasta qué punto los usuarios pueden asegurarse que es debido y acorde a la normativa vigente?

Nuestra ley 19.628 no regula la transferencia internacional de datos personales. El proyecto de ley originario presentado por la Cámara de Diputados contenía un artículo 23°[202]: "Prohíbase a los responsables de bancos de datos personales transmitir datos personales desde países o con destino a

[202] Historia de la ley 19.628, disponible en www.bcn.cl.

países cuya legislación no ofrezca garantías análogas a las previstas en esta ley. Se exceptúan las transferencias internacionales de créditos, las transferencias de información para los efectos de prestar colaboración a las autoridades judiciales y policiales internacionales, así como cualquier otra transferencia que resulte de la aplicación de tratados o convenios internacionales en que el estado de Chile sea parte". Sin embargo, la Comisión Mixta rechazó el precepto debido a que consideró que la regulación de la transferencia internacional de datos correspondía ser efectuada por tratados internacionales sobre la materia.

En Chile, no existe un órgano que controle y fiscalice el tratamiento llevado a cabo por terceros, en ese sentido no se garantiza la protección a las personas. Desconocemos si las filiales pueden ser consideradas seguras, no sabemos la naturaleza de los datos transmitidos, la finalidad de la transmisión, la duración del tratamiento o los tratamientos previstos, ni las medidas de seguridad que protejan los datos de trasferencias sucesivas.

Frente a la cláusula de jurisdicción de aplicación de las leyes de California EEUU, en Chile nada se ha discutido y no existe pronunciamiento al respecto por lo que se acepta tácitamente la establecida por Google, a pesar que nuestras legislaciones contienen grandes diferencias.

La normativa que protege los datos personales en Europa es adecuada y contiene armas legales le permiten hacer presión a Google para que adecue su política de privacidad. En Julio, Italia ha avisado a Google que debe ceñirse a las leyes locales en los próximos 18 meses si no quiere atenerse a multas de un millón de euros.

"Entre las medidas que tendrá que tomar está la necesidad de pedir permiso expreso al usuario para crear un perfil conjunto con todos sus datos; tendrá dos meses para borrar nuestros datos de sus servidores si decidimos no aceptarlo, y seis meses para borrar cualquier copia de seguridad que tuviese. En la solicitud de permiso Google tendrá que decir explícitamente al usuario que usará sus datos con propósito comercial."[203] Lamentablemente, Chile está lejano a poder realizar este tipo de presiones.

[203] OMICRONO. Italia obliga a Google a cambiar la manera en la que usa nuestros datos. [en línea] <http://www.omicrono.com/2014/07/italia-obliga-a-google-a-cambiar-la-manera-en-la-que-usa-nuestros-datos> [consulta: 27 julio 2014]

7. Consagración jurisprudencial del "Derecho al olvido". Sentencia del Tribunal de Justicia Europeo

El martes 13 de abril del presente año se dio a conocer la sentencia del Tribunal de Justicia Europeo[204] que estableció la responsabilidad de Google a retirar enlaces de información personal de sus búsquedas, si así se lo solicitan, consagrando el derecho al olvido en internet en Europa.

El juicio se produjo por la reclamación de Mario Costeja a la Agencia Española de Protección de Datos, quién al buscar su nombre en el motor de búsqueda Google obtenía como resultado dos vínculos hacia páginas del periódico La Vanguardia en las que figuraba un anuncio de un subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social vinculadas a su nombre.

La Agencia de Protección de datos desestimó la reclamación en contra del medio de comunicación, al considerar que la publicación estaba legalmente justificada, dado que había sido ordenada por orden del Ministerio del Trabajo y Asuntos Sociales y tenía por objeto dar la máxima publicidad a la subasta para conseguir la mayor ocurrencia de licitadores. En cambio, estimó que la petición

[204] INFOCURIA. Jurisprudencia del Tribunal de Justicia. [en línea] <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=260957> [consulta: 17 de abril 2014]

que se dirigía contra Google Spain y Google INC debía ser acogida plateándole al Tribunal de Justicia Europeo cuestionamientos prejudiciales.

En este sentido, la Corte declaró que el motor de búsqueda es responsable del tratamiento de datos cuando esta contiene información personal, ya que su actividad consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, cumpliendo lo establecido en la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

Por otro lado, cuando el gestor del motor de búsqueda crea en el Estado miembro de la comunidad europea, una sucursal o filial destinada a garantizar la promoción y venta de espacios publicitarios y cuya actividad se dirige a sus habitantes, debe considerarse como un establecimiento responsable del tratamiento. Lo que significa que la directiva europea de protección de datos y las normas nacionales de transposición son aplicables extraterritorialmente a empresas ubicadas en países no miembros de la Unión Europea.

Por esto está obligado a eliminar de la lista de resultados obtenidos, tras una búsqueda efectuada a partir del nombre de una persona, vínculos a páginas web publicadas por terceros y que contienen información relativa a ella,

incluso aunque estas no se borren previa o simultáneamente de las páginas web y aunque esta publicación sea lícita, ya que el derecho a la vida privada y protección de datos personales prevalecen no sólo sobre el interés económico del gestor del motor de búsqueda sino también sobre el interés del público de acceder a la información que verse sobre una persona.

Según la Corte el motor de búsqueda permite, mediante una lista de resultados, una visión estructurada de la información relativa a una persona ya que esta se interconecta permitiendo formar un perfil detallado, afectando mayormente los derechos fundamentales que lo que haría un editor de página web. “Google es un “controlador” cuando se trata de procesamiento de datos en sus servidores y la “actividad de los buscadores es adicional a la de los editores de sitios web”[205]

Este fallo es un gran triunfo de la protección a privacidad y datos personales frente a los gigantes de la tecnología informática (Google, Yahoo, Microsoft), pero encierra una serie de cuestionamientos y dudas pues no se pronuncia sobre el fondo del asunto que tiene que ver con los contenidos y no con los enlaces.

[205] PULSO. Histórico fallo sobre privacidad golpea a las empresas de internet en EEUU. [en línea] <http://www.pulso.cl/noticia/portada/ft/2014/05/22-43312-9-historico-fallo-sobre-privacidad-golpea-a-las-empresas-de-internet-en-eeuu.shtml> [consulta: 21 de abril 2014]

“Según el presidente de la Asociación de Internautas, Víctor Domingo, la sentencia otorga mayor poder a Google y le da una responsabilidad "que no se merece" como decidir qué enlaces a informaciones perjudican o no a los ciudadanos.”[206]

Frente a las miles de solicitudes de retiro de información, Google desarrolló un formulario online disponible para los usuarios europeos que permite denunciar enlaces potencialmente nocivos para su persona, que no erradicará la información sino que comenzará un proceso de investigación y comprobación, teniendo en cuenta el “interés legítimo”.

Las personas deben “entregar su nombre, un correo de contacto y explicar detalladamente cuál es su relación con el contenido que se quiere eliminar y por qué puede ser considerado "irrelevante, desactualizado o inapropiado”.[207]

Sin duda, deberá revisarse caso a caso ya que el proceso de recopilación de información está automatizado y es casi imposible detectar los

[206] LA RAZÓN DIGITAL. Un hito en la defensa de la privacidad. [en línea] <http://www.larazon.es/detalle_normal/noticias/6349235/un-hito-en-la-defensa-de-la-privacidad#Ttt17bnb9k4u7cgs> [consulta: 19 de abril 2014]

[207] EMOL. Google habilita formulario online para que europeos pidan la eliminación de contenido. [en línea] <http://www.emol.com/noticias/tecnologia/2014/05/30/662777/google-habilita-formulario-online-para-que-europeos-pidan-la-eliminacion-de-contenido.html> [consulta: 30 de mayo 2014]

enlaces que puedan vulnerar la resolución europea. También debe tomarse en cuenta el papel que la persona desempeñe en la vida pública.

"Hasta el momento, la tecnología por sí sola no permite todavía comprobar de forma masiva y automática si el enlace que se pide borrar realmente perjudica al denunciante o si el caso está entre los supuestos que ampara la ley para acogerse al "derecho al olvido". Depende del contexto"[208]

¿Cuál será el criterio a aplicar? Grave es que algunos se vinculen con procesos criminales: "un hombre que intentó matar a su familia (…) persona condenada por posesión de imágenes de abuso infantil (…) político que quiere postular a la reelección y posee mala imagen, entre otros"[209]

La gestión de Google de las peticiones del "derecho al olvido" de los ciudadanos europeos ha sido cuestionada después de que el buscador restringiera el borrado de los enlaces en Internet solo a las páginas web europeas, lo que significa que cualquiera puede acceder fácilmente a la misma información cambiando al buscador google.com.[210]

[208] LA INFORMACIÓN.COM. Google dispone de robots para borrar datos, pero no para verificarlos en masa. [en línea] <http://noticias.lainformacion.com/ciencia-y-tecnologia/tecnologia-general/google-dispone-de-robots-para-borrar-datos-pero-no-para-verificarlos-en-masa_IMfiaRtAAT947SUjkjl3C3/> [consulta: 21 de abril 2014]
[209] METAGNIA. Google se prepara para un aluvión de demandas de olvido en internet. [en línea] http://www.metagnia.com/2014/05/18/6197 [consulta: 18 de abril 2014]
[210] El ECONOMISTA. Google de nuevo cuestionada en la UE por la sentencia sobre la privacidad. [en línea] <http://www.eleconomista.es/cultura/noticias/5966847/07/14/Google-de-

La controversia materializa el conflicto de derechos que se produce entre la protección a la privacidad frente al derecho a la información y libertad de expresión, que la sentencia del Tribunal pretende balancear estableciendo que los únicos casos en que los datos no pueden ser borrados es cuando se trate de figuras púbicas o el acceso esté justificado por el interés social.

En junio, la Corte Suprema de la provincia canadiense de Columbia Británica tomó una decisión en torno a un juicio por espionaje industrial, ordenándole al buscador que dejara de mostrar sitios entre sus resultados de búsqueda.

La empresa accedió a hacerlo a través de Google Canadá, pero la Corte decidió que la solución se implementara a nivel mundial, algo a lo que Google se negó, argumentando que "equivaldría a una orden a nivel mundial que no podría hacerse cumplir y porque constituiría una intromisión injustificada en las actividades comerciales de Google como motor de búsqueda".[211]

Como podemos percatarnos, las consecuencias derivadas de este fallo, son aún difíciles de precisar.

---

nuevo-cuestionada-en-la-UE-por-la-sentencia-sobre-la-privacidad.html#.Kku8l31WRKkCREY> [consulta: 28 julio 2014]

[211] FAYERWAYER. Google pierde apelación y lo obligan a borrar a empresa canadiense. [en línea[<http://www.fayerwayer.com/2014/07/google-pierde-apelacion-y-lo-obligan-a-borrar-a-empresa-canadiense/> [consulta: 28 julio 2014]

CONCLUSIONES

Tenemos derecho de abstraernos del control social, sin embargo en la “sociedad de la información” no es tan sencillo. Actualmente, es fácil violar la vida privada de una persona pues existen instrumentos que permiten hacerlo: una forma directa es mediante el reconocimiento audiovisual o a través de métodos de investigación que permitan suministrar información acerca de la persona; y un método indirecto es a través de la recolección, comparación o agregación de datos, que son procesados por medio de un computador.

Las tecnologías de la información al permitir el manejo rápido y eficiente de gran cantidad de datos facilitan el almacenamiento automático, constituyéndose en una verdadera fuente de poder. La web permite además, transferir esta información a una velocidad infinita.

Internet junto con hacer más difícil el control sobre la difusión de datos personales, ha complicado la seguridad sobre la exactitud de dicha información, que se almacena o transmite para distintos fines. El mal uso puede conllevar a manipulaciones, persecuciones, presiones, asedios o discriminaciones, tanto del gobierno como entes privados.

Los datos personales son el motor de la nueva economía de Internet. El modelo tradicional de la publicidad está rápidamente dando paso a un nuevo mundo digital, que hace coincidir los anuncios con el lector o el espectador. Al navegar por la web, las cookies actúan como un identificador único. Permiten a las páginas realizar un seguimiento de lo que el usuario está viendo, almacenando esa información en sus sistemas para construir un perfil de intereses personales.

Google unido a la brecha informática existente, acrecienta las posibilidades de afectar el derecho a la privacidad, pues existe ignorancia sobre el valor de los datos entregados o simplemente no se tiene conocimiento de la utilización de ellos por agentes inescrupulosos.

Las personas no están plenamente conscientes de que están pagando con sus datos personales los servicios gratuitos entregados por Google, pero establecer prohibiciones legales a este tipo de modelo de negocios puede afectar el avance tecnológico y la invención.

El problema es ¿quién define, decide y marca los límites de la utilización de nuestros datos personales? Mientras la legislación chilena no delimite qué no se pueden traspasar, lo hace el propio Google.

Si bien la sentencia del Tribunal de Justicia Europea estableció el derecho a solicitar la eliminación de información indexada de páginas web cuando esta vulnere el derecho a la vida privada y protección de datos personales, sólo será aplicable a países en que rija la Directiva 95/46/CE del Parlamento Europeo y del Consejo, así como el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, es decir, países de la Unión Europea, donde el estándar normativo de protección a los derechos fundamentales es mucho mayor que en nuestro país.

La empresa solicita el consentimiento de la persona antes de utilizar sus datos para cualquier fin distinto de los establecidos en la política de privacidad, pero ¿qué pasa cuando el usuario acepta sin leer? Es responsabilidad propia, pero de igual forma las condiciones de privacidad son largas, lo que requiere tiempo, y en un lenguaje árido, provocando que el usuario en su afán de rapidez, acepte sin miramientos y sin percatarse del riesgo que puede correr su información personal.

Hay diversos problemas que debilitan la capacidad de los individuos de realizar elecciones informadas y racionales respecto de los costos y beneficios de consentir en la recolección, uso y divulgación de los datos personales; e incluso al estar adecuadamente informados, no se puede anticipar con exactitud los beneficios o riesgos de eventuales usos posteriores.

El individuo debe tener derecho a conocer y tener acceso a las instituciones que manejan datos relativos a su persona, y sobre cuál es el tipo de información que poseen. En caso que la información sea errónea, inexacta o incluso irrelevante, la persona puede solicitar una modificación o alteración de ella, pues el uso de la información debe ser conforme al fin por el cual se proveyó.

A pesar de la solicitud del usuario de actualización, modificación o eliminación de datos incorrectos en los registros del servicio de Google, la compañía conserva los datos y las copias residuales no se destruyen de inmediato, quedando almacenadas en los servidores activos y copias de seguridad ¿Cuál es la duración de mantención de los datos? El criterio debería ser que la voluntad del titular predominara sobre los intereses privados.

Los medios informáticos deben garantizar una entrega de información sobre la recopilación de datos personales que sea clara y explícita para los motivos que desean utilizarla.

Para evitar toda la problemática de utilización de datos personales, debe reconocerse jurídicamente la facultad del individuo a decidir cuándo y cómo está dispuesto a permitir que sea difundida su información. La persona debe saber expresamente de qué se trata, cuales son los motivos y en qué se

utilizarán sus datos (esto claramente conlleva una educación ciudadana acerca del tratamiento de sus datos personales). Sólo de esta forma se puede controlar y conocer los datos que sobre ella se encuentre en soportes informáticos pues se le está reconociendo una tutela legal para conocer y acceder a las informaciones almacenadas en archivos de datos que les conciernen.

Normas para obtener nuevamente el consentimiento para otros usos de los datos ya entregados, podrían resultar muy costosas o servir de barreras de entrada a la innovación, obteniendo resultados no deseado para la sociedad y la mayoría de las personas. Pero un consentimiento en blanco, que permita un uso ilimitado puede resultar peligroso y dañino si es utilizado de forma que la gente no pueda entender o anticipar.

La ley debe evaluar y entregar lineamientos sobre los nuevos tipos de uso de datos, en el momento que se presenten. Algunos deberán ser absolutamente restringidos, limitados, requerir nueva manifestación de consentimiento, permitidos pero con el derecho a revocar el consentimiento, o permitidos sin nueva autorización.

Un contexto institucional favorable a una regulación eficaz de datos personales debería contar con una ley básica que contenga principios generales, normas específicas destinadas a regular los conflictos que se

plantean, un órgano independiente con funciones de supervisión y reglamentación, un sistema que permita la intervención del Poder Judicial por vía de recursos.

Es necesario e importante realizar esfuerzos para mejorar la autogestión de la privacidad a través de más educación a los consumidores, más avisos destacados y más instancias para manifestar el consentimiento. De esta forma se avanzaría en concientizar a las personas acerca de la importancia del tratamiento de datos que realiza Google y se evitarían usos maliciosos o inadecuados de la información personal. Serán los mismos usuarios quienes vigilen y supervisen la actividad realizada por el gigante tecnológico.

Finalmente, cabe señalar que en julio de 2014, el Ministerio de Economía, Fomento y Turismo, ha presentado a consulta pública un anteproyecto de ley que da forma a un Sistema de Protección de Datos sustentado en el derecho de las personas de controlar y proteger su información, de manera de evitar que sus derechos sean afectados por el tratamiento de datos.[212]

[212] MINISTERIO DE ECONOMÍA, FOMENTO Y TURISMO. Ante proyecto de Ley Protección de las Personas del Tratamiento de Datos Personales. [en línea] <http://www.participacionciudadana.economia.gob.cl/consultas-ciudadanas-virtuales/ante-proyecto-de-ley-proteccion-de-las-personas-del-tratamiento-de> [consulta: 27 de julio 2014]

BIBLIOGRAFÍA

Leyes:

- CHILE. Ministerio Secretaría General de la Presidencia. 1999. Ley 19.628: Sobre protección de la vida privada. Modificado por la ley 20.521, del 23 de julio de 2011. Art. 9 inciso 3.

- CHILE. Ministerio Secretaría General de la Presidencia. 2008. Ley 20.285: Sobre acceso a la información pública. Art 33 m)

- CHILE. Ministerio Secretaría General de la Presidencia. 2005. Decreto 100: Fija el texto refundido, coordinado y sistematizado de la Constitución Política de la República de Chile.

- CHILE. Ministerio de Justicia. 1996. Ley 19477: Aprueba Ley Orgánica Del Servicio De Registro Civil e Identificación.

Libros y Publicaciones:

- ALDUNATE Lizana, Eduardo. 2007. Panorama actual del amparo y hábeas corpus en Chile. Chile. Estudios Constitucionales, Año 5 N° 1, ISSN 0718-0195, Universidad de Talca.

- ALVARADO, Francisco. 2013 Internet y las fuentes de acceso público a datos personales. Memoria para optar al título de Licenciado en Ciencias jurídicas y Sociales. Universidad de Chile.

- ANGUITA Ramírez, Pedro. 2007. La protección de datos personales en el derecho y la vida privada. Régimen jurídico, jurisprudencia y derecho comparado. Editorial Jurídica de Chile.

- BANDA Vergara, Alfonso. 2000. Manejo de datos personales, un límite al derecho a la vida privada. Universidad Austral de Chile. 59 p.

- BARROS Bourie, Enrique. 1998. Honra, privacidad e información: un crucial conflicto de bienes jurídicos. Año 5- 1998. Coquimbo. Revista de Derecho, Universidad Católica del Norte Sede Coquimbo.

- CARILLO, Marc. 2003. El derecho a no ser molestado. Información y vida privada. Navarra: Colección Divulgación Jurídica. Thomson Aranzadi.

- CERDA Silva, Alberto. 2003. La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales. Tesis de Magister. Facultad de Derecho, Universidad de Chile.

    - 2003. Autodeterminación informativa y leyes sobre protección de datos. Revista Chilena de Derecho informático. No. 3 Diciembre 2003.

    - 2008. Hacia un modelo integrado de regulación y control en la protección de datos personales. Revista Derecho y Humanidades Nº 13 / 2008/ 121 -130.

    - 2002. Intimidad de los trabajadores y tratamiento de datos personales por empleadores. Revista chilena en derecho informático. [en línea] <http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/viewFile/10645/10921> [consulta: 19 junio 2014]

- CORRAL Talciani, Hernán. 2000. Configuración Jurídica del Derecho a la Privacidad I: Origen, desarrollo y fundamentos. Vol. 27 Nº 1. Chile. Revista Chilena de Derecho. Selección Estudios.

    - 2000. Configuración jurídica del derecho a la privacidad II: concepto y delimitación. Volumen 27 Nº 2. Chile. Revista Chilena de Derecho, Sección Estudios.

    - 2001. La vida privada y la propia imagen como objetos de disposición negocial. Chile. Revista Chilena de Derecho, Universidad Católica del Norte, Nº8.

- DÍAZ Tolosa, Regina. 2007. Delitos que vulneran la intimidad de las Personas: Análisis crítico del artículo 161-A del Código Penal Chileno. Chile. Revista Ius et Praxis, 13 (1): 291 – 314.

- FROSSINI, Vittorio. 1983. Los derechos humanos en la sociedad tecnológica. Anuario de Derechos Humanos, número 2.

- HERVADA, Javier. 1993. Los derechos inherentes a la dignidad de la persona humana. En Escritos de Derecho Natural. 2º Edición. Pamplona. EUNSA.

- JERVIS Ortíz, Paula. 2002 Derechos del titular de datos y habeas data en la ley 19.628. Ponencia pronunciada en el “Seminario de Datos Personales en Chile. El Nuevo Régimen Normativo, organizado por el Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de chile, entre los días 30 de septiembre y 14 de octubre de 2002.

- JIJENA Leiva, Renato. 1992. Chile, la protección penal de la Intimidad y el delito informático. Editorial jurídica de Chile. Santiago de Chile. 1ª edición.

    - 2010 Actualidad de la protección de datos personales en América Latina. El caso de Chile. Revolución Informática con independencia del individuo.

    - 2010. Actualidad de la protección de datos personales en América Latina. El caso Chile. Memorias del XIV Congreso Iberoamericano de Derecho e Informática. Monterey. UNAM.

- LOVERA Parmo, Domingo. 2009. El interés público como estándar. Libertad de expresión y vida privada. Universidad Diego Portales. [en línea] <http://www.derechoshumanos.udp.cl/wp-content/uploads/2009/07/interes-publico.pdf> [consulta: 09 junio 2014].

- LYON Puelma, Alberto. 1993. Teoría de la personalidad. Chile. Ediciones Universidad Católica de Chile.

- MEINS Olivares Eduardo. 2000. Derecho a la Intimidad y a la Honra en Chile. Año/ Vol. 6, Nº 001. Talca Chile. Universidad de Talca. Ius et Praxis.

- NOGEIRA Alcala, Humberto. 2003. Reflexiones sobre el establecimiento constitucional del hábeas data y el proyecto de ley en tramitación parlamentaria sobre la materia. Año 3 Nº1. Talca. Ius Et Praxis. Universidad de Talca. Facultad de Ciencias Jurídicas y Sociales.

    - 2007. El derecho a la propia imagen como derecho fundamental implícito. fundamentación y caracterización. Chile. Revista Ius et Praxis, 13 (2): 245-285.

    - 1981. El derecho a la información en el ámbito del Derecho Constitucional chileno y comparado en Iberoamérica y Estados Unidos.

- PEÑA González, Carlos. Informe sobre el proyecto de ley de protección del honor y la intimidad de las personas.

- PÉREZ-LUÑO, Antonio Enrique. 1989. Los Derechos Humanos en la sociedad tecnológica", en Cuadernos y Debates, Centro de Estudios Constitucionales, Madrid, núm. 21.

    - 1989. Los derechos humanos en la sociedad tecnológica. Número 12. Madrid. Cuadernos y debates, Centro de Estudios Constitucionales.

- QUEZADA Rodríguez, Flavio. 2012. La protección de Datos Personales en la Jurisprudencia del TC. Vol. 1 Nº 1. Chile. Revista Chilena de Derecho y Tecnología.

- REISCHL, Gerald. 2008. El engaño Google. Una potencia mundial incontrolada en Internet. Primera Edición. España. Medialive Content, S.L.

- SOLEVE, Daniel J. 2013. La autogestión de la privacidad y el dilema del consentimiento. En: Revista Chilena de Derecho y Tecnología. Centro de Estudios en Derecho Informático. Universidad de Chile. Vol. 2 Num. 2.

- SUAREZ Crothers, Christian. 2000. El concepto de derecho a la vida privada en el derecho anglosajón y europeo. Revista de Derecho. Vol. XI. Universidad de Talca.

- SUAREZ Sánchez-Ocaña, Alejandro. 2012. Desnudando a Google. La inquietante realidad que no quieren que conozcas. Madrid. Deusto.

- VIAL Solar, Tomás. 2000. Hacia la construcción de un concepto constitucional del derecho a la vida privada. Volumen XVI Nº3. Chile. Revista Persona y Sociedad.

Páginas web:

- 20 MINUTOS. Expertos informáticos detectan un fallo de seguridad en Android [en línea] <http://www.20minutos.es/noticia/1053847/0/fallo/seguridad/android/> [consulta: 10 enero 2012]

- ADSLZONE. Google será finalmente juzgada por el caso “Streetview”. <http://www.adslzone.net/2014/07/02/google-sera-finalmente-juzgada-por-el-caso-streetview/> [consulta: 03 julio 2014]

- BIT-TECH. Google admits Street View WiFi sniffing. 2014. [en línea] <http://www.bit-tech.net/news/bits/2010/05/17/google-admits-street-view-wifi-sniffing/1> [consulta: 14 enero 2012]

- CHROME. Obtén un navegador web gratuito y veloz. [en línea] <https://www.google.com/intl/es-419/chrome/browser/?hl=es-419&brand=CHMI> [consulta: 8 enero 2012]

- CHROME. Una renovada perspectiva sobre los navegadores. [en línea] <http://www.google.com/chrome/intl/es-419/why.html> [consulta: 8 enero 2012]

- C-Net. Gmail edges Hotmail as world's top e-mail service. 2012. [en línea] <http://news.cnet.com/8301-1023_3-57543177-93/gmail-edges-hotmail-as-worlds-top-e-mail-service/> [consulta: 8 enero 2012]

- CNN. YouTube blocked in China. 2009. [en línea] <http://edition.cnn.com/2009/TECH/ptech/03/25/youtube.china/index.html> [consulta: 9 enero 2012]

- CYBERLAW CLINIC. Una demanda por violación de la privacidad frena la red Google Buzz de Gmail [en línea] <http://cyberlaw.ucm.es/expertos/loreto-corredoira/81> [consulta: 9 enero 2012]

- DERECHOS DIGITALES. Sobre el monitoreo de Internet por el Gobierno. [en línea] <https://www.derechosdigitales.org/2085/sobre-el-monitoreo-de-internet-por-el-gobierno/> [consulta: 03 julio 2014]

- El ECONOMISTA. Google de nuevo cuestionada en la UE por la sentencia sobre la privacidad. [en línea] <http://www.eleconomista.es/cultura/noticias/5966847/07/14/Google-de-

nuevo-cuestionada-en-la-UE-por-la-sentencia-sobre-la-privacidad.html#.Kku8l31WRKkCREY> [consulta: 28 julio 2014]

- EL FINANCIERO. Revisar las políticas de privacidad de redes sociales puede tomar 180 horas. [en línea] <http://www.elfinanciero.com.mx/empresas/revisar-las-politicas-de-privacidad-de-redes-sociales-puede-tomar-180-horas.html> [consulta: 30 de mayo 2014].

- FAYERWAYER. Google pierde apelación y lo obligan a borrar a empresa canadiense. [en línea[<http://www.fayerwayer.com/2014/07/google-pierde-apelacion-y-lo-obligan-a-borrar-a-empresa-canadiense/> [consulta: 28 julio 2014]

- EL MUNDO. Obama autorizó a la NSA a aprovechar 'agujeros' en Internet para proteger la seguridad nacional 2014. [en línea] <http://www.elmundo.es/internacional/2014/04/13/534ac004268e3ec46d8b4572.html> [consulta: 15 abril 2014]

- EL MUNDO. YouTube deberá bloquear los vídeos musicales en Alemania. 2009 [en línea] <http://www.elmundo.es/elmundo/2009/04/02/navegante/1238656149.html> [consulta: 9 enero 2012]

- EMOL. Google habilita formulario online para que europeos pidan la eliminación de contenido. [en línea] <http://www.emol.com/noticias/tecnologia/2014/05/30/662777/google-habilita-formulario-online-para-que-europeos-pidan-la-eliminacion-de-contenido.html> [consulta: 30 de mayo 2014]

- EMOL. Tailandia bloquea a YouTube por videos que se burlan del rey. 2007. [en línea] http://www.emol.com/noticias/tecnologia/2007/04/04/251598/tailandia-bloquea-a-youtube-por-videos-que-se-burlan-del-rey.html [consulta: 9 enero 2012]

- GOOGLE EMPRESA. Lo que creemos. Puedes hacer dinero sin hacer el mal [en línea] <https://www.google.cl/intl/es-419/about/company/philosophy/> [consulta: 05 junio 2014]

- GOOGLE PRIVACY POLICY GETS PUBLIC AIRING. 2012 [en línea] <http://www.ft.com/cms/s/2/7d8c375c-6489-11e1-9aa1-00144feabdc0.html#axzz1qDtzQOJh> [consulta: 12 agosto 2012]

- GOOGLE. Acerca de la verificación en dos pasos. [en línea] <https://support.google.com/accounts/answer/180744?hl=es-419&rd=1> [consulta: 01 abril 2014]

- GOOGLE. Búsqueda SSL. [en línea] <http://support.google.com/websearch/bin/answer.py?hl=es&answer=173733> [consulta: 14 enero 2012]

- GOOGLE. Cómo administrar cookies y datos de sitios. [en línea] <http://support.google.com/chrome/bin/answer.py?hl=es&answer=95647> [consulta: 12 enero 2013]

- GOOGLE. Como retirar contenido de Google [en línea] <https://support.google.com/legal/troubleshooter/1114905?rd=2> [consulta: 09 de abril del 2014]

- GOOGLE. Condiciones del servicio de Google [en línea] <https://www.google.cl/intl/es-419/policies/terms/regional.html> [consulta: 09 abril 2014]

- GOOGLE. El blog corporativo de Google para América Latina. [en línea] <http://googleamericalatinablog.blogspot.com/2014/04/ampliamos-los-servicios-de-seguridad-de.html> [consulta: 11 abril 2014]

- GOOGLE. Informe de Transparencia [en línea] <http://www.google.com/transparencyreport/userdatarequests/countries/> [consulta: 03 de julio 2014]

- GOOGLE. Informe de transparencia. Solicitudes de información acerca de nuestros usuarios. [en línea] <http://www.google.com/transparencyreport/userdatarequests> [consulta: 3 abril 2014]

- GOOGLE. La misión de Google es organizar la información del mundo y hacerla universalmente accesible y útil. [en línea] <https://www.google.cl/intl/es/about/company/> [consulta: 12 agosto 2012]

- GOOGLE. Las diez razones principales para utilizar Gmail [en línea] <https://mail.google.com/mail/help/intl/es/about.html> [consulta: 8 enero 2012]

- GOOGLE. Marcos de autorregulación de Google. [en línea] <https://www.google.com/intl/es/policies/privacy/frameworks/> [consulta: 14 enero 2012]

- GOOGLE. Más información sobre Gmail y la privacidad [en línea] <https://mail.google.com/mail/help/intl/es/more.html> [consulta: 8 enero 2012]

- GOOGLE. Nuestros productos y servicios. [en línea] <https://www.google.cl/intl/es/about/company/products/> [consulta: 12 agosto 2012]

- GOOGLE. Políticas de Privacidad de Google. [en línea] <https://www.google.cl/intl/es/policies/privacy/> [consulta: 07 de abril 2014]

- HEATHBLEED. Heathbleed bug. [en línea] <http://heartbleed.com/> [consulta: 03 julio 2014]

- INFOCURIA. Jurisprudencia del Tribunal de Justicia. [en línea] <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=260957> [consulta: 17 abril 2014]

- LA INFORMACIÓN.COM Google dispone de robots para borrar datos, pero no para verificarlos en masa. [en línea] <http://noticias.lainformacion.com/ciencia-y-tecnologia/tecnologia-general/google-dispone-de-robots-para-borrar-datos-pero-no-para-verificarlos-en-masa_IMfiaRtAAT947SUjkjl3C3/> [consulta: 21 abril 2014]

- LA NACIÓN. Google suma alertas para mejorar la seguridad en Android [en línea] <http://www.lanacion.com.ar/1679657-google-suma-alertas-para-mejorar-la-seguridad-en-android> [consulta: 11 abril 2014]

- LA RAZÓN DIGITAL. Un hito en la defensa de la privacidad [en línea] <http://www.larazon.es/detalle_normal/noticias/6349235/un-hito-en-la-defensa-de-la-privacidad#Ttt17bnb9k4u7cgs> [consulta: 19 abril 2014]

- LA SEGUNDA. Trabajo policial usa cada vez más los datos de Facebook para atrapar delincuentes. [en línea] <http://www.lasegunda.com/Noticias/Nacional/2014/06/942158/trabajo-policial-usa-cada-vez-mas-los-datos-de-facebook-para-atrapar-delincuentes> [consulta: 03 julio 2014]

- LA VOZ DE GALICIA. Turquía reabre YouTube tras más de dos años de bloqueo. 2010. [en línea] <http://www.lavozdegalicia.es/tecnologia/2010/10/31/00031288523645938566654.htm> [consulta: 9 enero 2012]

- MASTER PLAN THE MOVIE [en línea] <http://masterplanthemovie.com/> [consulta: 10 diciembre 2013]

- METAGNIA. Google se prepara para un aluvión de demandas de olvido en internet. [en línea] http://www.metagnia.com/2014/05/18/6197 [consulta: 18 de abril 2014]

- MINISTERIO DE ECONOMÍA, FOMENTO Y TURISMO. Ante proyecto de Ley Protección de las Personas del Tratamiento de Datos Personales. [en línea] <http://www.participacionciudadana.economia.gob.cl/consultas-ciudadanas-virtuales/ante-proyecto-de-ley-proteccion-de-las-personas-del-tratamiento-de> [consulta: 27 de julio 2014]

- MIS RESPUESTAS. ¿Qué son los buscadores en Internet? [en línea] <http://www.misrespuestas.com/que-son-los-buscadores-en-internet.html> [consulta: 8 enero 2012]

- MODMYMOBILE. Las aplicaciones de Android enviarían información GPS a los anunciantes [en línea] <http://modmymobile.com/forums/552-general-android-esp/557091-las-aplicaciones-de-android-enviarian-informacion-gps-los-anunciantes.html> [consulta: 08 abril 2014]

- NOTICIAS MVS. Permanecerá YouTube bloqueado en Turquía. 2014 [en línea] <http://www.noticiasmvs.com/#!/noticias/permanecera-youtube-bloqueado-en-turquia-330.html> [consulta: 21 de abril del 2014]

- OMICRONO. Italia obliga a Google a cambiar la manera en la que usa nuestros datos. [en línea] <http://www.omicrono.com/2014/07/italia-obliga-a-google-a-cambiar-la-manera-en-la-que-usa-nuestros-datos> [consulta: 27 julio 2014]

- PULSO. Histórico fallo sobre privacidad golpea a las empresas de internet en EEUU. [en línea] <http://www.pulso.cl/noticia/portada/ft/2014/05/22-43312-9-historico-fallo-sobre-privacidad-golpea-a-las-empresas-de-internet-en-eeuu.shtml> [consulta: 21 abril 2014]

- REGISTRO CIVIL. [en línea] <www.registrocivil.cl/f_banco_de_datos.html> [consulta: 27 diciembre 2012]

- RT QUESTION MORE. Google's Eric Schmidt: NSA spying 'outrageous' 2014. [en línea] <http://rt.com/usa/google-schmidt-nsa-outrageous-195/> [consulta: 15 abril 2014]

- RT QUESTIONS MORE. Google encrypts Gmail to safeguard against NSA snooping. 2014. [en línea] <http://rt.com/news/google-gmail-encryption-nsa-297> [consulta: 15 abril 2014]

- TELAM. Google paga una multa de un millón de euros por violar la privacidad. [en línea] <http://www.telam.com.ar/notas/201404/57994-google-paga-una-multa-de-millon-de-euros-por-violar-la-privacidad.html> [consulta: 04 abril 2014]

- THE NEW YORK TIME. Google Zooms In Too Close for Some. [en línea] <http://www.nytimes.com/2007/06/01/technology/01private.html?_r=0> [consulta: 07 julio 2014]

- WIRED. Google Takes Wi-Fi Snooping Scandal to the Supreme Court. Kevin Poulsen [en línea] <http://www.wired.com/2014/04/threatlevel_0401_streetview/> [consulta: 04 abril del 2014]

- YOUTUBE. Público y orientación en YouTube. [en línea] http://www.youtube.com/t/advertising_audience_targeting [consulta: 9 enero 2012]

Proyectos de ley:

- CHILE. Tramitación de Proyectos Congreso Nacional. 2000. Boletín 2474-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2000. Boletín 2600-18
- CHILE. Tramitación de Proyectos Congreso Nacional. 2001. Boletín 2735-05
- CHILE. Tramitación de Proyectos Congreso Nacional. 2001. Boletín 2771-05
- CHILE. Tramitación de Proyectos Congreso Nacional. 2002. Boletín 3003-19
- CHILE. Tramitación de Proyectos Congreso Nacional. 2002. Boletín 3066-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2002. Boletín 3094-19
- CHILE. Tramitación de Proyectos Congreso Nacional. 2002. Boletín 3095-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2003. Boletín 3185-19
- CHILE. Tramitación de Proyectos Congreso Nacional. 2003. Boletín 3312-05

- CHILE. Tramitación de Proyectos Congreso Nacional. 2004. Boletín 3656-18
- CHILE. Tramitación de Proyectos Congreso Nacional. 2005. Boletín 3796-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2005. Boletín 3773-06
- CHILE. Tramitación de Proyectos Congreso Nacional. 2006. Boletín 4124-18
- CHILE. Tramitación de Proyectos Congreso Nacional. 2006. Boletín 4124-18
- CHILE. Tramitación de Proyectos Congreso Nacional. 2006. Boletín 4143-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2006. Boletín 4203-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2006. Boletín 4429-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2006. Boletín 4466-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2006. Boletín 4482-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2006. Boletín 4629-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2006. Boletín 4436-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2007. Boletín 4959-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2007. Boletín 4972-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2007. Boletín 5009-06
- CHILE. Tramitación de Proyectos Congreso Nacional. 2007. Boletín 5053-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2007. Boletín 5122-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2007. Boletín 5309-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2007. Boletín 5320-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2007. Boletín 5351-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2007. Boletín 5356-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2007. Boletín 5365-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2008. Boletín 5754-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2008. Boletín 5883-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2008. Boletín 5999-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2008. Boletín 6120-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2008. Boletín 6298-05
- CHILE. Tramitación de Proyectos Congreso Nacional. 2009. Boletín 6353-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2009. Boletín 6495-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2009. Boletín 6594-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2009. Boletín 6598-06
- CHILE. Tramitación de Proyectos Congreso Nacional. 2009. Boletín 6800-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2010. Boletín 6854-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2010. Boletín 6914-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2010. Boletín 6939-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2010. Boletín 6979-06
- CHILE. Tramitación de Proyectos Congreso Nacional. 2010. Boletín 6982-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2010. Boletín 6994-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2010. Boletín 7026-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2010. Boletín 7055-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2010. Boletín 7093-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2010. Boletín 7132-03

- CHILE. Tramitación de Proyectos Congreso Nacional. 2010. Boletín 7158-05
- CHILE. Tramitación de Proyectos Congreso Nacional. 2010. Boletín 7232-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2010. Boletín 7282-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2010. Boletín 7392-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2011. Boletín 7715-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2011. Boletín 7732-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2011. Boletín 7776-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2011. Boletín 7777-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2011. Boletín 7794-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2011. Boletín 7808-13
- CHILE. Tramitación de Proyectos Congreso Nacional. 2011. Boletín 7831-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2011. Boletín 7833-13
- CHILE. Tramitación de Proyectos Congreso Nacional. 2011. Boletín 7864-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2011. Boletín 7886-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2011. Boletín 8086-04
- CHILE. Tramitación de Proyectos Congreso Nacional. 2012. Boletín 8143-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2012. Boletín 8175-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2012. Boletín 8208-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2012. Boletín 8222-11
- CHILE. Tramitación de Proyectos Congreso Nacional. 2012. Boletín 8275-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2012. Boletín 8559-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2012. Boletín 8589-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2014. Boletín 9242-10
- CHILE. Tramitación de Proyectos Congreso Nacional. 2014. Boletín 9252-15
- CHILE. Tramitación de Proyectos Congreso Nacional. 2014. Boletín 9388-03
- CHILE. Tramitación de Proyectos Congreso Nacional. 2014. Boletín 9384-07
- CHILE. Tramitación de Proyectos Congreso Nacional. 2014. Boletín 9308-07

Jurisprudencia:

- CORTE INTERAMERICANA DE DERECHOS HUMANOS. 2011. Caso Fontevecchia y D`Amico Vs. Argentina. Fondo, Reparaciones y Costas.
- CORTE SUPREMA. 2011. Recurso de Protección. Sentencia Rol 10180-10.
- CORTE SUPREMA. 2011. Recurso de Protección. Sentencia Rol 10944-11.
- CORTE SUPREMA. 2012. Recurso de Protección. Sentencia Rol 1661-12.
- CORTE SUPREMA. 2012. Recurso de Protección. Sentencia Rol 3500-12.
- CORTE SUPREMA. 2013. Recurso de Protección. Sentencia Rol 3538-13.
- CORTE SUPREMA. 2014. Recurso de Protección. Sentencia Rol 3816-14.
- CORTE SUPREMA. 2014. Recurso de Protección. Sentencia Rol 6337-14.

- TRIBUNAL CONSTITUCIONAL. 2008. Sentencia Rol N° 1185.
- TRIBUNAL CONSTITUCIONAL. 2013. Sentencia Rol 2513-13.
- TRIBUNAL CONSTITUCIONAL. 2013. Sentencia Rol 2422.
- TRIBUNAL CONSTITUCIONAL. 2013. Sentencia Rol 2454-13.