LA PROTECCIÓN DEL DERECHO A LA VIDA PRIVADA EN INTERNET Y OTROS MEDIOS DE COMUNICACIÓN ELECTRÓNICOS

(BORRADOR DE TESIS PARA OPTAR AL GRADO DE LICENCIADO EN DERECHO)

PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

PROFESOR GUÍA: MIGUEL ÁNGEL FERNÁNDEZ GONZÁLEZ
ALUMNO: FELIPE FRANCISCO CORONEL CARCELÉN

A mi familia ecuatoriana,
a mi familia chilena,
a Chile, mi segunda Patria

INTRODUCCIÓN

Todo ser humano, desde que nace hasta que muere, tiene una vida interior. En ella es que van floreciendo los sentimientos o pensamientos que más tarde irán dándole forma a la personalidad de cada individuo. Se trata de aquella parte de nuestras vidas que, por esencia, no le pertenece a nadie más que a nosotros mismos, donde se guardan celosamente aspectos muy íntimos y propios de cada uno, y que de compartirse, se lo hace dentro de nuestro círculo más familiar y cercano. De ella han ido derivando necesidades de todo hombre como el ser dejado en paz y en soledad para vivir consigo mismo, o el que no se revelen hechos que le pertenecen porque forman parte de sus secretos personales. Es el derecho a *tener* y a *vivir* nuestra vida privada, un derecho de tal jerarquía que en una sociedad que se rige por los principios de la democracia, su desarrollo y protección son fundamentales a la hora de buscar el bien común. "Los profetas, decía Wiston Churchill, provienen necesariamente de la civilización, pero todo profeta ha debido retirarse al desierto....y debe, cada cierto tiempo, buscar la soledad y absorverse en la meditación. Esta es la manera como se fabrica la dinamita mental"[1].

Sin embargo, el derecho a la vida privada de las personas definitivamente en los últimos tiempos ha ampliado su ámbito de ejercicio. Y es que se trata de un derecho que ha ido evolucionando, producto de una sociedad donde el conocer la vida íntima de los demás se vuelve día a día en un desafío para algunos y en un negocio para otros. Muchos han señalado que el desarrollo de la tecnología ha traído consigo el desarrollo de métodos para invadir nuestra vida interior. Creo que no se equivocan, y precisamente uno de esos nuevos métodos los constituye el más poderoso medio de comunicación que ha inventado el hombre: Internet, que ha dado nacimiento a la llamada *Sociedad de la Información*. Aquellos que conocen la novela de Orwell *"1984"* habrán escuchado hablar del "Gran Hermano", una especie de ojo que se encarga de registrar todos los pasos que damos en nuestra vida cuotidiana. Aún cuando en la actualidad no hemos llegado a ese extremo de control, no hay duda que sí existen entidades con tendencias *orwelianas*, que amenazan nuestro derecho fundamental a tener una vida privada. No en vano el español Antonio Pérez Luño ha manifestado que se trata

[1] Citado por Pierre KAISER, La protection de la vie privée, Presses Universitaires d'Aix-Marseille, 2e Edition, 1990, pág. 4, traducción libre.

de uno de los derechos humanos más vulnerados en la actualidad. El desafío por estudiar este fenómeno ha sido el motivo que ha dado pie a las siguientes páginas.

Desde esta perspectiva, en la primera parte de este trabajo se analizará como ha ido evolucionando el derecho a la vida privada de los hombres desde civilizaciones antiguas, como la griega y la romana, pasando por la influencia del cristianismo, del pensamiento filosófico de la edad media, de su posterior desarrollo en ordenamientos jurídicos y en la jurisprudencia, de su reconocimiento como derecho fundamental, y de cómo se lo entiende en la actualidad. Ello ha venido de la mano de toda una evolución conceptual que no nos ha sido indiferente y que ha merecido estudiarse con detalle a través de las diversas consideraciones que este derecho ha acarreado.

Ha sido importante también conocer acerca del resguardo que el mundo del derecho le ha otorgado a la intimidad de los seres humanos. Con esta idea hemos pretendido analizar el derecho comparado, por medio de Tratados Internacionales, Constituciones, normas internas, y proyectos de ley que, concientes de la amenaza que representan las nuevas tecnologías, han querido resguardar información perteneciente a nuestra esfera íntima. De la misma manera, se ha hecho también un estudio profundo sobre la protección del derecho a la vida privada a lo largo de todo el ordenamiento jurídico chileno.

En una segunda parte hemos pretendido darle una mirada a cómo han sido asimiladas las nuevas tecnologías en el mundo del derecho. Producto de ello, se ha estudiado especialmente a Internet, su historia, su definición, sus características y su evolución; a más de otras nuevas tecnologías derivadas de la aplicación de este nuevo medio de comunicación.

Explicado esto, se ha querido exponer cuales son las principales amenazas y violaciones que Internet ha traído consigo frente al derecho de toda persona a que no se conozcan aspectos o datos de carácter personal, pertenecientes a su vida privada. Para ello, se ha debido recurrir a jurisprudencia internacional (y a la escasísima jurisprudencia chilena) y a noticias sobre este ámbito que han dado cuenta de las inclinaciones de distintos sistemas normativos para afrontar el problema.

Con el objeto de que este trabajo sea lo más completo posible, finalmente hemos expuesto las principales soluciones que se han puesto sobre el tapete. Para ello, hemos querido que éstas sean conocidas desde dos perspectivas: una tecnológica y otra jurídica.

Primera Parte

Reflexiones acerca del Derecho a la Vida Privada

CAPÍTULO I: EVOLUCIÓN HISTÓRICA Y CONCEPTUAL DEL DERECHO A LA VIDA PRIVADA

El hombre, desde siempre, se ha desarrollado en un entorno dentro del cual, parte de su tiempo lo ha dedicado a sí mismo. Tiempo de reflexión, de recogimiento, de paz, de soledad, de reserva, que se manifiesta desde prácticamente la toma de razón del ser humano. Pues bien, a medida que el hombre se va desarrollando, también hace dentro de sí todo un mundo interno que a lo largo de su existencia irá construyendo lo que es su vida propia, su vida íntima, su vida interna, aquella parte de su ser que será celosamente resguardada para sí mismo, su **vida privada**.

Esta parte de la vida de las personas sin duda alguna que ha ido evolucionando con el transcurso de la historia de la humanidad, si bien porque cada vez se ha vuelto más preciado proteger esta parte de la integridad de las personas, todo ello debido a las constantes amenazas que el desarrollo del hombre ha acarreado. Desde esta perspectiva, se hará un breve análisis de cómo ha evolucionado esta parte íntima de la esfera humana, pues ya nadie niega que el concepto de vida privada ha evolucionado de manera radical en relación a sus primeras manifestaciones, tema que será tratado a continuación.

Evolución Histórica de la protección de la vida privada

De la Edad Antigua a la Edad Moderna

Las primeras manifestaciones respecto a la vida íntima de las personas se remontan a la Edad Antigua. En la época de los griegos, el desarrollo de la intimidad de las personas fue bastante limitado en el sentido de que la legislación de la época no favoreció mucho a la distinción entre vida pública y vida privada. "En Grecia no se entendía una separación entre lo público y lo propio de cada individuo, en consecuencia, esta concepción de ciudadanía del mundo griego influyó negativamente en la construcción del mundo familiar y personal pues, los aspectos más interiores de la vida humana quedaban a merced del Estado y sus leyes. Si bien no era posible la configuración de un derecho a la intimidad tal como en la actualidad se entiende, ello no significaba que no existiera, sino que era eficazmente reprimido por la exigencia de participación en la vida de la polis. Como consecuencia de las luchas internas entre las polis, la idea de ciudadanía tan arraigada en el pueblo griego, sufrió un grave quebranto que fue mitigado con el surgimiento de sociedades religiosas que encontraron su máximo exponente en el Cristianismo".[2]

[2] Federico Rafael MOEYKENS y Carlos Eduardo SALTOR en Argentina: La protección de Datos Personales en el Proyecto de Código Civil unificado con el Código de Comercio de la República Argentina, pág. 2, de texto publicado en http://publicaciones.derecho.org/redi/No._23_-_Junio_del_2000/9, visitado en diciembre de 2001.

En la sociedad ateniense, una filosofía parecida cobró también relevancia en el sentido de que la importancia del hombre se vio reflejada en relación a su participación en los asuntos de la polis, vale decir, en los asuntos públicos. De esta manera, es posible afirmar el valor que se les daba a las personas según su vida externa, más precisamente la vida pública que llevaban, dejando de lado la importancia del desarrollo de su vida interna.

Sin embargo, con la llegada del mundo romano, el desarrollo de la vida privada de las personas adquirió mucho más relevancia ya que se consideraba que era un medio a través del cual los hombres conocían su propio mundo interior, una manera de alcanzar su propia esencia. En este proceso de desarrollo del concepto de vida privada, se dan las primeras pautas de su reconocimiento jurídico.

"El reconocimiento del derecho a la intimidad estaba dado por la protección jurídica del domicilio y la correspondencia, entre otros, aunque tal vez el fundamento se encontraba en la seguridad y el orden público. No obstante, se evidenció en algunas normas legales, el desprecio del mundo romano por la intimidad de la persona, por ejemplo en la ilegalidad de los matrimonios entre personas de edad avanzada o en el adulterio considerado como delito de acusación pública.

Pero en definitiva, la idea de intimidad estaba presente entre los romanos y adquirió mayor significación que la que tuvo en el mundo griego"[3].

Algunos historiadores afirman que el período comprendido entre el fin del imperio romano hasta el año mil está marcado por la llegada del cristianismo y porque se considera como "el cambio entre el hombre cívico hacia el hombre interior", lo cual se vivió primeramente en las catacumbas, y después cuando justamente el cristianismo se convertiría en la religión oficial del imperio. Es con la llegada del mundo cristiano que el reconocimiento de la intimidad se descubre como sustancia del alma. "Tú, cuando quieras rezar, ve a la pieza más alejada, y cierra la puerta..." diría el Evangelio.[4] Se propaga al encuentro del hombre y de su relación con el Ser Supremo. "La culminación del pensamiento medieval cristiano está dado por Santo Tomás de Aquino, la filosofía escolástica admite la existencia de bienes que están en la persona, en su mismo cuerpo, y que ella consiste en la conciencia que cada uno de nosotros tiene como sujeto irrepetible"[5]. San Agustín también es partidario del recogimiento personal, entendiendo a la intimidad como autoconciencia de la subjetividad. De esta manera, el desarrollo de la vida interna de las personas formaría parte sin duda de su desarrollo espiritual.

Con la disgregación de la Sociedad Feudal, los individuos se ven mucho más ligados al hecho de vivir en sociedad, vinculándose mucho más entre sí, y haciendo de su vida cotidiana una vida en comunidad a través de la creación de los grupos feudales. Ello trajo como consecuencia también la necesidad del hombre de reservarse un espacio para sí mismo, y esto se vio reflejado en el pasaje de la confesión pública a la confesión

[3] Ibídem, pág. 3.

[4] Mateo, 20.

[5] Paulina ZÚNIGA LIRA, El Derecho a la Intimidad y la Protección de Datos de Carácter Personal, Tesis de Grado de la Facultad de Derecho de la Pontificia Universidad Católica de Chile, 1999, pág. 5.

individual, e incluso, en el hecho de que los siervos compraran su derecho a casarse libremente . No sería sino con la llegada de la burguesía que la intimidad se transforma en una necesidad colectiva. Debemos partir de la base que la idea de intimidad estaba guardada solamente para un selecto grupo de personas, por lo cual nace la inquietud de hacerla llegar a los sectores más humildes de la sociedad. [6]

Según relata Raúl García Aspillaga, el primer antecedente sobre el origen del **derecho** a la intimidad se encuentra en una sentencia dictada en 1348 en Inglaterra. "Según algunos datos recogidos, el demandado de aquel remoto caso fue una noche a la taberna de los demandantes para comprarles vino. Encontrando la puerta cerrada, comenzó a golpearla con un hacha pequeña que llevaba. La tabernera se asomó a la ventana (baja según parece) y le dijo que cesara de golpear la puerta. Lo que ocurrió después no está muy claro, porque no se sabe a ciencia cierta si el demandado solamente continuó golpeando la puerta o también trató de alcanzar a la mujer. El resultado es que se concedió una indemnización por daños y perjuicios, aunque la taberna no recibiese ningún golpe. Y se concedió esa indemnización porque un "mal" se había cometido.¿Qué mal? Desde el momento en que no existió agresión, sólo podía tratarse de una extensión de la protección dada a la persona, un reconocimiento del derecho a la intimidad".[7] Pocos años más tarde, en 1356, se comenzaría a considerar la buena fama y la posición social, apareciendo las leyes de difamación y libelo.[8]

Del Renacimiento al Siglo de Las Luces:

Entre el período que va desde el Renacimiento hasta el Siglo de Las Luces, tomaría forma paralelamente la aparición de la vida pública de las personas y el desarrollo de los servicios del Estado, los cuales indirectamente aportaron a la construcción de la vida privada de las personas a través de la difusión de textos que, gracias a la imprenta, a la alfabetización y la lectura, hicieron en el hombre de la época que el recogimiento y la reflexión formen parte de su vida. La burguesía culta formaba pequeños grupos dedicados a discutir temas importantes, dentro de los cuales se consideró mucho a la vida familiar como un lugar privilegiado para alcanzar momentos de intimidad.[9] En este sentido, la Revolución Francesa, por medio de la Declaración de los Derechos del Hombre y del Ciudadano, no haría sino consolidar estas ideas a través del reconocimiento de "derechos naturales e imprescriptibles de todo hombre", anunciados en el artículo segundo de dicha Declaración, como los derechos de asociación, de propiedad, de libertad.

---

[6] Ver sobre este tema la obra de Pierre KAISER, La protection de la vie privée, Presses Universitaires d'Aix-Marseille, 2e Edition, 1990, pág. 4.

[7] Raúl GARCÍA ASPILLAGA, La vida privada y la intimidad de las personas, Tesis de Grado de la Facultad de Derecho de la Pontificia Universidad Católica de Chile,1988, pág. 91. Ver también la famosa obra de Samuel WARREN y Louis BRANDEIS, El derecho a la intimidad, Editorial Civitas, Madrid, 1995, pág. 22, donde se señala, refiriéndose brevemente a este caso que "a partir de la acción por agresión se llegó a la acción por amenaza", citando también en la misma obra a *Anuario*, Lib. Ass., Folio 99, pl. 60 (1348 ó 1349), parece ser el primer caso documentado en el que se estableció una indemnización por coacción, pág. 22, nota 1.

[8] Citado por Samuel WARREN y Louis BRANDIES, El derecho a la intimidad, pág. 23, nota 3.

[9] Pierre KAISER, La protection de la vie privée, Presses Universitaires d'Aix-Marseille, 2e Edition, 1990, pág. 4.

No deja de ser rescatable el alcance que muchos filósofos vieron en la importancia de resguardar la intimidad de las personas. En la Filosofía del Derecho, autores como Hobbes, Locke, Price y Stuart Mill escribieron al respecto. Hobbes, aunque defendió siempre el absolutismo, comienza ya a pensar en la existencia de una esfera privada mínima en su obra *Leviatán*. Locke por su parte desarrolla en su *Ensayo sobre el Gobierno Civil* las ideas de libertad y autonomía, excluyendo cualquier sometimiento a la voluntad arbitraria de otro; y en *Carta sobre la Tolerancia* ya introduce la idea de exclusión de la intervención del Estado y su administración en el marco de la vida privada. Según Price, los americanos lucharon por cuatro libertades principales cuyo principio latente era la noción de "autodirección" o "autogobierno". Finalmente, Stuart Mill escribió en *Sobre la Libertad* ideas relativas al individuo como centro de la moral y receptáculo de la libertad. Según describe Castillo Marcano, refiriéndose a este último, "…sin utilizar la terminología de 'vida privada', 'privacidad' o 'intimidad' (…) deja claro que debe existir una separación nítida entre el ámbito propio de cada individuo y la esfera pública."[10] Por su parte, Benigno Pendás, refiriéndose a la utilización del vocablo *privacy* por los filósofos Locke y Stuart Mill señala que "alcanzan momentos de excelencia cuando construyen con rara perfección un derecho exquisito: *to let be alone*".[11]

En todo caso, no serían los únicos intelectuales de la época que tratarían el tema, pues resulta interesante mencionar a otros filósofos como Benjamín Constante de Rebecque, Jeremy Bentham, o al francés Alexis de Tocqueville. Sin embargo, somos partidarios en pensar que el despegue del reconocimiento del derecho a la vida privada se produce definitivamente a principios del siglo XIX.

Ya en 1819, en la Cámara de Diputados Francesa, el tratadista Royer-Collard, al pronunciarse respecto del artículo 20 de un proyecto de ley sobre delitos cometidos por medio de la prensa se refería a la vida privada como "amurallada, protegida por un muro de los ataques del mundo exterior".[12] Y es en Francia precisamente donde se encuentra una interesante sentencia que se refiere justamente a la invasión de la intimidad de las personas, cuya importancia radica en el reconocimiento que hace de los aspectos de la viva pública y privada de las personas. Tiene su origen en un caso en el que se publicaron en un diario imágenes de una actriz difunta, Rachel Felix, cuando en realidad sus parientes querían que se guardara absoluta reserva de su cadáver. Reza la sentencia en una de sus partes que: "Considerando que el derecho a oponerse a esa reproducción es absoluto, que tiene su principio en el respeto que impone el dolor de las familias, y que no

---

[10] José Luis CASTILLO MARCANO, El Derecho a la Intimidad y la Protección de Datos Personales en el Derecho Español, En Boletín de la Academia de Ciencias Políticas y Sociales. Nº 134. Año LXIV, Caracas, 1997, pág. 8, de texto publicado en http://vlex.com/redi/No._37_-_Agosto_del_2001/5, visitada en enero del año 2002.

[11] Samuel WARREN y Louis BRANDEIS, El Derecho a la Intimidad, Editorial Civitas, Madrid, 1995, pág. 13, introducción de Benigno PENDÁS.

[12] Citado por Luis María MANTONI, en El derecho a la intimidad, Edit Trivium. Madrid, 1983, pág. 319. Ver también Raúl GARCÍA ASPILLAGA, La vida privada y la intimidad de las personas, Tesis de Grado de la Facultad de Derecho de la Pontificia Universidad Católica de Chile,1988,citando a Royer COLLARD, De la Liberté de Presse, (Discours), Paris, 1949, pág. 98. Al respecto leer también de Paulina ZÚÑIGA LIRA El derecho a la intimidad y la Protección de Datos de Carácter Personal, Tesis de Grado de la Facultad de Derecho de la Pontificia Universidad Católica de Chile, 1999, pág. 6.

podría desconocerse sin herir los sentimientos más íntimos y los más respetables de la naturaleza y de la piedad doméstica". [13]

De aquí se desprende también el reconocimiento que se hace a la protección del derecho a la vida privada de una persona fallecida, tomando en cuenta que respecto de este tema, parte de la doctrina considera que con el fin de la existencia humana, no procedería seguir protegiendo la privacidad del difunto.[14]

El 11 de mayo de 1868 se publicaría la Ley de Prensa de la República Francesa, (en francés *Loi relative à la presse*), la cual en su artículo 11 establecía que: "Toda publicación en un periódico relativa a un hecho de la vida privada constituye una falta que se castigará con una multa de 500 francos. La acción no podrá ser ejercida más que a instancias de la parte interesada" [15](subrayado es mío). Era la primera vez que la legislación francesa utilizaba el término "vida privada", lo cual representa un avance notable, aún cuando su alcance fuera vago. Sin lugar a dudas que la protección de este derecho comenzaría ya a tomar forma, y no será sino en 1890 cuando tome un giro de 180 grados al otro lado del mundo, con el célebre artículo de S. Warren y L. Brandeis, publicado el 15 de diciembre de aquel año, en el volumen IV, número 5 de la *Harvard Law Review* de los Estados Unidos.

---

[13] Citado por Miguel URABAYEN, Vida Privada e Información, pág. 152. Ver también el comentario de esta sentencia en una forma más extensa en el trabajo de Raúl García Aspillaga, La vida privada y la intimidad de las personas, Tesis de Grado de la Facultad de Derecho de la Pontificia Universidad Católica de Chile,1988, pág. 99.

[14] Como lo señala el propio GARCÍA ASPILLAGA,: "La jurisprudencia norteamericana más constante declara que el "Right of privacy" se extingue por la muerte de las personas, atendido su carácter personal; se afirma que el derecho muere con la persona. Diverso es, en general el criterio europeo, conforme al cual se estima que "la vida privada de las personas fallecidas está protegida al mismo título que la de las personas vivas, con la reserva de que los derechos de la historia son mayores y aumentan a medida que se retrocede en el tiempo". Para el propio García, la muerte de una persona trae consigo la extinción de su derecho a proteger su intimidad, por lo cual señala que "la intimidad y, consiguientemente, el derecho que la ampara, se extingue "ope legis", con la persona de su titular". (Raúl GARCÍA ASPILLAGA, La vida privada y la intimidad de las personas, Tesis de Grado de la Facultad de Derecho de la Pontificia Universidad Católica de Chile,1988, pág. 34). En el trabajo del mismo autor resulta interesante la cita que hace respecto de Robert Badinter, donde se señala que " a todas las razones que imponen la protección de la vida privada se añade en este momento el respeto debido a los muertos. Lo que no era tolerable en vida de la víctima, aparece menos soportable cuando ella ya no existe(...) Hay, sin embargo, un caso en que la vida privada de un individuo debe caer , después de muerto, en el dominio público. Es la suerte del hombre protagonista de la Historia ". Robert BADINTER, Le droit au respect del la vie privée, Jurisclasseur Périodique, 1968, V.I., N° 2136.
Resulta de gran interés considerar el alcance que le quiso dar la Comisión de Estudio de la Nueva Constitución al concepto de vida privada, protegiendo a las personas fallecidas, por lo cual en el artículo 19 n°4 la Constitución asegura a todas las personas "El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia"(subrayado es mío). En la Sesión 129, del 12 de junio de 1975, uno de los argumentos que se dio para proteger la intimidad de la familia es la protección y respeto de la honra de la persona difunta y de sus parientes. Es por ello que el señor ORTÚZAR declara que "parece evidente que el hecho de que una persona fallezca no autoriza para que el día de mañana pueda ser objeto de toda clase de difamaciones, sobre todo si ha sido respetable. Este derecho corresponde a su familia, especialmente a sus hijos, a su cónyuge"(Enrique EVANS DE LA CUADRA, Los Derechos Constitucionales, págs. 183 y 184). Esta postura sería adoptada también por los Senadores GUZMÁN y OVALLE. El autor de este trabajo concuerda con los argumentos recién mencionados. Así mismo, el proyecto de Ley de Protección Civil del Honor y de la Intimidad de las Personas también resguarda a los familiares del difunto, como se verá más adelante.

[15] La traducción al francés de este artículo es la siguiente: "Toute publication dans un écrit périodique relative à la vie privée constitue une contravention punie d'une amende de cinq cents francs.
La poursuite ne pourra être exercée que sur la plainte de la partie interessée". Riviere, Codes Français et Lois Usuelles, App. Code Penal, page 20.

De la Era Moderna a la Post-Moderna

Samuel Denis Warren (1852-1910), próspero y reconocido abogado de Boston, junto con Louis Dembitz Brandeis (1856-1946), primer judío que accedió en calidad de juez al Tribunal Supremo Federal, serían los autores de un clásico de la literatura jurídica, extremadamente rico en jurisprudencia de la época, *The Right to Privacy*, calificado por Benigno Pendás, traductor al español de esta obra como "un modelo prototípico del *Case Law*, de principios creados por vía inductiva a partir de precedentes"[16], del cual derivarían grandes pautas para la posterior evolución de este derecho.

Este texto tiene como antecedente directo la publicación del Juez norteamericano Thomas A. Cooley, quien en 1873 editaría su obra *The elements of Torts*, y cuya trascendencia se debe a la definición que el autor dio a la palabra "intimidad", entendida ésta como *the right to be let alone*, concepto que la doctrina tradicionalmente entiende en castellano como "el derecho a ser dejado en paz", o "el derecho a ser dejado a solas".[17]

Se dice que este derecho deriva del derecho a la propiedad, del cual Warren y Brandeis hacen una distinción entre los derechos a la propiedad materiales e inmateriales, éstos últimos considerados de amplio ámbito de aplicación, comprendiendo obviamente el derecho a la reserva, o a ser dejado solo [18]. Sin embargo, los autores van más allá de lo que la doctrina de la época entendía por propiedad privada, por lo que manifestarían que "El principio que ampara los escritos personales, y toda otra obra personal, no ya contra el robo o la apropiación, sino contra cualquier forma de publicación, no es en realidad el principio de propiedad privada, sino el de la inviolabilidad de las personas"(subrayado es mío).[19]

The right to be let alone nace como una respuesta a la constante amenaza que producían en la época los medios de comunicación como los diarios y revistas, respecto de su intromisión en la vida privada de las personas; y de la protección que un sistema como el *Common Law* debía ofrecer a sus ciudadanos. Así, los propios autores señalan que "El *common law* garantiza a cada persona el derecho a decidir hasta qué punto pueden ser comunicados a otros sus pensamientos, sentimientos y emociones" basando incluso este argumento en una sentencia pronunciada en 1759 por el juez J. Yates, respecto del caso entre Millar v/s Taylor donde se señalaba que "Es cierto que toda persona tiene derecho a reservarse sus sentimientos, si así lo desea. Tiene, ciertamente, derecho a juzgar si quiere hacerlos públicos o manifestarlos únicamente ante sus amigos".[20]

---

[16] Samuel WARREN y Louis BRANDEIS, El Derecho a la Intimidad, Editorial Civitas, Madrid, 1995, págs. 14 y 15.

[17] Citado por Miguel URABAYEN, Vida privada e información: un conflicto permanente, Ediciones Universidad de Navarra S.A., Pamplona, 1997, pág. 13.

[18] Ibídem, pag. 24.

[19] Ibídem, pág. 45.

[20] Ibídem, pág. 31.

La importancia de esta publicación radica en que comienzan a tomar forma los derechos de las personas frente a la protección de su vida privada, como por ejemplo el derecho a proteger su intimidad, el derecho a exigir la veracidad de lo que se publica, el derecho a la rectificación, la responsabilidad extracontractual que la violación de este derecho acarrea, por mencionar algunos.

El propio Louis D. Brandeis, casi 30 años más tarde, como Juez del Tribunal Supremo, entroncó el derecho a la intimidad en la IV enmienda de la Constitución en el voto particular que formuló a la sentencia Olmstead v. United States (1928). En aquella ocasión, se hablaría sobre la necesidad de crear leyes que sobrevivan al paso del tiempo, aspecto interesante puesto que demuestra que a principios del siglo pasado ya existía la conciencia del carácter cambiante de las realidades, y de la necesidad de crear normas que se adaptaran a tales cambios. Brandeis decía que las leyes deben ser capaces de una aplicación más amplia que la requerida por la transgresión que causó su redacción, añadiendo que "en la aplicación de una Constitución no es suficiente contemplar lo que ha sido o lo que es, sino lo que puede ser". Con respecto a la protección del derecho a la privacidad específicamente, el Juez Brandeis expresó que "El progreso que ha logrado la ciencia en su búsqueda para proveer al gobierno de medios para el espionaje no se detendrá con el invento de la intervención de teléfonos. Es posible que algún día se diseñen medios para que el gobierno pueda, sin remover los documentos de gavetas secretas, reproducirlos en las Cortes, y para que pueda exponer ante un jurado las incidencias más íntimas de un hogar."[21]

Resulta sumamente interesante la visión futurista de este juez, ya que prevee el uso de nuevos instrumentos análogos al teléfono para la intercepción de las comunicaciones privadas, manifestando que ello también constituye una violación de la quinta enmienda de la Carta Política de los Estados Unidos de América. Refiriéndose al espíritu de las normas establecidas específicamente en cuanto a la interpretación de la Cuarta y Quinta Enmiendas, el propio Brandeis ratificaría que "ellos quisieron proteger a los americanos en sus creencias, sus pensamientos, sus emociones y sus sensaciones. Ellos confirieron a los ciudadanos el derecho, oponible al gobierno, de ser dejados en paz, el más amplio de los derechos y el más valorado por los hombres civilizados. Para proteger ese derecho, cualquier invasión del gobierno a la privacidad del individuo que no esté justificada debe ser considerada como una violación de la Cuarta Enmienda, sin importar qué medios se hayan empleado. Asimismo, el uso de pruebas obtenidas mediante tales invasiones como evidencia en un juicio debe ser considerado una violación de la Quinta Enmienda."[22]

Durante la primera mitad del siglo XX, el derecho a la intimidad fue altamente vulnerado, consecuencia en gran parte de las dos guerras mundiales, ya que el ser humano comenzó a descubrir que la información sobre las personas era una herramienta extremadamente poderosa. La intromisión a la vida privada de los hombres

---

[21]Citado por Alexander ROSEMBERG HOLCBLAT y Moirah SÁNCHEZ SANZ, El derecho a la privacidad en Internet, pág. 9 de texto publicado en http://vlex.com/redi/No._37_-_Agosto_del_2001/5, visitado en enero de 2002.

[22] Ibídem, pág 10.

se tornó bastante más sofisticada de lo que se conocía hasta entonces. Un ejemplo claro de ello fue el sistema de identificación que se utilizó en algunos países europeos como Holanda, donde los dígitos que conformaban la cédula nacional de identidad clasificaban a las personas según diversos factores como su origen, sexo, raza, etc... Entre 1940 a 1943, la GESTAPO descubrió en este sistema un excelente método para clasificar a las personas, lo cual tuvo definitivamente consecuencias macabras.

"La codificación utilizaba la primera de las trece cifras del número nacional de identidad, donde nos hemos acostumbrado a no ver más que los valores 1 (hombres) ó 2 (mujeres). De hecho, esta primera cifra puede tener diez valores y ser transformada en indicador de sexo y de la raza. El número en cuestión tendría entonces un significado del tipo siguiente: 1 (hombre ario), 2 (mujer aria), 3 (hombre judío), 4 (mujer judía), etc.(...) Cabe considerar el caso de Holanda, que disponía ya de un número nacional de identidad antes del año 1940, del mismo tipo que Francia quiso instituir en el año 1942, por suerte demasiado tarde. La existencia de este sistema significante de identificación es uno de los elementos que explican el hecho de que prácticamente el 100 por cien de los judíos holandeses fueran reconocidos, arrestados y deportados. Hasta tal punto eso es cierto que, aprendida la lección de esa experiencia, la administración holandesa se vale ahora de un número totalmente no significativo, con una tabla de correspondencia entre los nombres y esos números situada en un lugar minado que se puede hacer saltar por los aires en caso de invasión."[23]

Después de este período, que marcó una de las páginas más negras de la historia de la humanidad, el derecho a la vida privada de las personas tuvo una evolución trascendental: fue reconocido internacionalmente como **derecho humano** en la Declaración Universal de Derechos Humanos de la Organización de las Naciones Unidas, celebrada en París el 10 de diciembre de 1948. Según el jurista francés Pierre Kaiser "El reconocimiento del respeto de la vida de las personas como un derecho humano en las nuevas Declaraciones de derechos posteriores a la Segunda Guerra Mundial es el resultado de una doble evolución en la concepción de este derecho. Inicialmente concebidos como derechos necesarios para la *vida* del hombre en sociedad, se extenderán, en estas nuevas Declaraciones, como derechos necesarios para su *desarrollo*, es decir, siguiendo la definición del Presidente Cassin, quien tanto contribuyó en esto, como el conjunto de derechos y facultades sin las cuales el ser humano no puede desarrollar plenamente su personalidad".[24] (traducción libre).

---

[23]Amílcar MENDOZA LUNA, Los Cookies ¿Amenaza a la privacidad de información en la Internet?, citando a GALLOUEDEC-GENUYS, Francoise & LEMOINE, Philippe y a Margarita Gabriela PRIETO ACOSTA, Informática Jurídica: el derecho ante un gran reto, Bogotá: Pontificia Universidad Javeriana. 1984. P.104, en texto publicado en http://vlex.com/redi/No._30_-_Enero_del_2001/8, visitado en enero de 2002.

[24] PierreKAISER, La protection de la vie privée, Presses Universitaires d'Aix-Marseille, 2e Edition, 1990, págs 8 y 9. La traducción de este extracto fue hecha por mí, cuyo texto original en francés es el siguiente: "La reconnaissance du respect de la vie privée comme un droit de l'homme dans les nouvelles Déclarations de ces droits qui ont suivi la deuxième guerre mondiale, est le résultat d'une double évolution dans la conception de ces droits. Initialement conçus comme droits nécessaires à la *vie* de l'homme en société, ils sont étendus, dans ces nouvelles Déclarations, aux droits nécessaires a son *développement*, c'est-à-dire, suivant la définition du Président Cassin, qui a beaucoup contribué a cette extensión, à l' ensemble des droits et des facultés sans lequels l' être humain ne peut développer pleinement sa personnalité".

A la Declaración Universal de los Derechos del Hombre le siguieron un sinnúmero de Tratados Internacionales que confirmaron y desarrollaron la protección de la vida privada de las personas, incluso incluyéndola en una gran cantidad de Constituciones alrededor del mundo, tema que será tratado con más detalle en el próximo capítulo de este trabajo.

Al momento de considerar al derecho al la vida privada como un derecho fundamental, surgió dentro del ámbito doctrinario todo un debate en cuanto a cómo éste debía ser clasificado. Tradicionalmente, los derechos humanos ha sido clasificados como de primera, segunda y tercera generación. Esta clasificación, según parte de la doctrina, responde al hecho de que los derechos del hombre sufren algunas mutaciones a través del tiempo. Como consecuencia de ello, se ha considerado que el proceso evolutivo que afronta la sociedad humana debe estar acompañado paralelamente con un proceso de evolución también jurídico. Desde este punto de vista, se consideran "derechos de primera generación" a las libertades individuales y sus derechos de defensa a través de la autolimitación y la no injerencia de los poderes públicos en la esfera privada.[25] También se conoce a este tipo de derechos como "derechos individuales", definidos por Eduardo Novoa Monreal como "aquellos que corresponden a los seres humanos por el solo hecho de ser tales, aun sin considerar su pertenencia a una organización determinada"[26]. Para este autor, el derecho a la vida privada se encuentra dentro de ésta categoría, opinión que comparte gran parte de la doctrina.

Son derechos de segunda generación –surgidos tras el desarrollo de luchas sociales–, derechos de participación que requieren de políticas activas de los poderes públicos encaminadas a garantizar su ejercicio, es decir, son derechos de tipo económico, social y cultural. Se los llama también derechos sociales, a "aquellos que el hombre puede reclamar del estado o de la sociedad como conjunto organizado en razón de estar incorporados a ellos y como un medio para un mejor desarrollo propio y de la comunidad de la que forma parte".[27] Dentro de este tipo de derechos están el derecho a la libertad de recepción y de divulgación de información.

En cuanto a los derechos de tercera generación, según Pérez Luño responden al fenómeno de la "contaminación de las libertades", que alude a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de la tecnología. Dentro de los rasgos innovadores de esta fase menciona el hecho de que la solidaridad constituye el valor guía de los derechos, porque se hallan aunados entre sí por su incidencia universal en la vida de todos y para realizarse exigen esfuerzos y responsabilidades comunes a escala mundial. [28] Esta última clasificación ha tenido gran aceptación por parte de la doctrina internacional.

---

[25] Rodolfo HERRERA BRAVO, Chile: ¿Por qué la Protección de Datos Personales es una garantía básica de los Derechos fundamentales?, pág. 2, de texto publicado en http://vlex.com/redi/No._38_-_Septiembre_del_2001/14, visitada en enero de 2002.

[26] Eduardo NOVOA MONREAL, Derecho a la vida privada y Libertad de Información, Siglo XXI Editores SA de CV, México D.F., cuarta edición, 1989, pág. 18.

[27] Ibídem.

Respecto de estos derechos fundamentales de tercera generación, Vittorio Frosini –mencionado por Sánchez Bravo[29] – señala que están estrechamente vinculados a la sociedad tecnológica, en su calidad de derechos positivos, por lo que ya no pueden calificarse de "innatos".

Emilio Suñé Llinás, por su parte, vincula estos derechos de tercera generación con los valores inherentes a la cultura postmaterialista, que ya no responden a la necesidad de seguridad física o económica, como en las dos generaciones anteriores, sino que se relacionan con la autorrealización personal, adoptando un carácter más expresivo que instrumental. [30]

Dentro de la doctrina chilena, no deja de ser interesante la opinión de María Carolina Ortúzar Villaroel, quien señala que " Estos derechos humanos de tercera generación son el producto de la reivindicación de ciertos nuevos valores (...). Dentro de esta categoría de los derechos humanos de la tercera generación es que se inserta el derecho a la intimidad frente a la nueva realidad social moderna que nos toca vivir, en tanto que se aspira a potenciar el valor de la privacidad del individuo en una sociedad caracterizada por una creciente densidad de las relaciones e interdependencias sociales"[31] , postura que es compartida por el autor de este trabajo, considerando la complejidad que comprende el contenido del derecho a la vida privada y su constante evolución.

Existen también aquellos que consideran al derecho a la vida privada como un "derecho de la personalidad"[32], sobre todo dentro de las legislaciones alemana y francesa. Los germanos, durante mucho tiempo rechazaron a este derecho como perteneciente a los derechos de la personalidad, pero en 1949, el artículo primero de la ley fundamental de la República Federal Alemana considera a la dignidad de la persona humana como *sagrada*. Uno de sus grandes aportes es que reconoce la indemnización por daño moral, producto de amenazas y violaciones a derechos de la personalidad como el derecho a la vida privada de las personas.

[28] Antonio E PÉREZ LUÑO; Mario LOSANO, María Fernanda GUERRERO, Libertad informática y leyes de protección de datos personales, Centro de Estudios Constitucionales. Madrid-España. 1989. p. 144.

[29] Álvaro SÁNCHEZ BRAVO, La protección del derecho a la libertad informática en la Unión Europea, Universidad de Sevilla, Secretariado de publicaciones. Sevilla-España. 1998. p. 35.

[30] Emilio SUÑE LLINÁS, Tratado de Derecho Informático, Vol. I, Universidad Complutense, Madrid-España. 2000, p. 31.

[31] María Carolina ORTÚZAR VILLAROEL, El nuevo concepto de Derecho a la Intimidad y su protección en la era tecnológica, Tesis de grado de la Escuela de Derecho de la Universidad Católica de Valparaíso, 1996, pág. 14.

[32] Tomás VIAL SOLAR, citando a Carlos PEÑA en El derecho a la vida privada y a la libertad de expresión en las constituciones de Chile y España: una propuesta de criterios de análisis, Tesis para optar al grado de Magíster en derecho público de la Facultad de Derecho de la Pontificia Universidad Católica de Chile,1997, define a los derechos personales como "derechos fundamentales respecto a los demás derechos del ordenamiento jurídico, sirviendo de presupuesto a los demás, lo que problematiza inusitadamente la posibilidad de un tratamiento dogmático normal por parte de la doctrina privatista", pág. 122.

En cuanto a la legislación francesa, otro ícono de la historia de la intimidad lo ha marcado el artículo 1382 de su Código Civil, en el que se consagra el deber de indemnizar por los daños efectuados, y que daría pie a la responsabilidad extracontractual. Dicho artículo señala que : "Cualquier hecho de una persona que cause daño a otra, obliga a la persona por cuya culpa se produjo el daño a repararlo"[33]. Es el reconocimiento de una acción civil por parte de la judicatura francesa frente a los daños causados por la invasión a la intimidad de las personas. Es lo que la doctrina, entre ellos el francés Pierre Kaiser, llama la "Teoría de la responsabilidad subjetiva o base de culpa".[34]

En Francia mismo, el 17 de julio de 1970 entraría en vigencia la Ley 70-643, cuyo objetivo sería "fortalecer las garantías protectoras de los derechos fundamentales"[35], y dentro de estas garantías estaba justamente la necesidad de reforzar la protección del derecho al secreto y a la vida privada de sus ciudadanos.

De estos antecedentes nacería el actual artículo noveno del Código Civil galo, que establece que: "Todos tienen derecho al respeto de su vida privada. Los jueces pueden, sin perjuicio de la reparación del daño sufrido, disponer de todas las medidas, como secuestro, incautación y otras, apropiadas para impedir o hacer cesar un atentado contra la intimidad de la vida privada; estas medidas pueden, en caso necesario, ser ordenadas en procedimiento de urgencia".[36] Es una novedad el hecho de que se le faculte al magistrado para tomar medidas precautorias como el secuestro, pero esto es el reflejo de una política que busca garantizar el cumplimiento que la responsabilidad extracontractual establece.

Dentro de la jurisprudencia germana, una de las sentencias más celebres es la del año 1983, donde se consagra el concepto de "autodeterminación informativa", que más tarde tendría gran aplicación a nivel doctrinal y que consolidaría toda una nueva teoría sobre la protección del derecho a la vida privada. Ella tiene su origen en una demanda que se interpuso ante el Tribunal Constitucional Federal, producto de la dictación de una ley que ordenaba realizar un censo general de la población. De ello, se pretendía obtener una base indispensable para las decisiones políticas, económicas y sociales del Estado. Sin embargo, este método de obtención de dicha información era considerado como atentatorio contra los derechos fundamentales de sus habitantes. En consecuencia, dicho Tribunal suspendió la realización del censo mediante una resolución provisional dictada con fecha 13 de abril de 1983. Allí se indicaba que " El derecho a la *autodeterminación informativa* deriva conjuntamente del principio de la dignidad de la persona, que actúa con autodeterminación al formar parte de una sociedad libre". Refiriéndose a la libertad y a la dignidad de las personas, "de la autodeterminación se debe deducir básicamente por sí misma cuándo y dentro de qué límites procede revelar

---

[33] Artículo 1382 del Código Civil Francés.

[34] Ver al respecto Eduardo NOVOA MONREAL, Derecho a la vida privada y Libertad de Información, Siglo XXI Editores SA de CV, México D.F., cuarta edición, 1989, pág. 27 . Ver también al respecto la obra de José Luis CEA EGAÑA, Vida pública, vida privada y derecho a la información: acerca del secreto de reserva, Revista de Derecho, Facultad de Ciencias Jurídicas y Sociales, Universidad Austral, Vol. III, N° 1-2, diciembre de 1992, pág. 14.

[35] Pierre KAISER, La protection de la vie privée, Presses Universitaires d'Aix-Marseille, 2e Edition, 1990, pág. 79.

[36] Artículo 9 del Código Civil de la República de Francia.

situaciones referentes a la propia vida(...). Sería contrario a dicha facultad de autodeterminación un orden social y un orden jurídico en el que el ciudadano ya no pudiera saber quién, qué, cuándo y con qué motivo se sabe algo sobre él. Esto no solo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental del funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos". [37]

Resulta sumamente interesante observar que sobre todo a partir de la segunda mitad del siglo XX, se comenzaron a utilizar y desarrollar muchos medios para invadir y transmitir datos concernientes a la vida propia de las personas. Tal es el caso de medios de comunicación como la prensa, la radio o la televisión, y posteriormente Internet. Ello trajo como consecuencia un vuelco trascendental al momento de proteger la vida privada de las personas. En poco tiempo se comenzó a comprender que una serie de datos concernientes a la vida personal de las personas, sin aparente importancia u orden se volvían un bien valioso y cotizado al ser clasificados, ordenados y condensados en bases de datos. Era el nacimiento de una nueva era en la invasión de la vida íntima de las personas: la era de la *libertad informática*, de la *autodeterminación informativa* y del *Habeas Data*. Comenzaba así mismo una nueva batalla para los defensores de aquella esfera íntima de la vida de las personas, una batalla contra el procesamiento de datos personales y una campaña por regular su tratamiento que hasta la fecha no ha terminado.

Según Renato Jijena Leiva, "La respuesta doctrinaria ha sido la **formulación de un nuevo concepto del Derecho a la Intimidad**, que surge frente a la llamada o reclamada *Libertad Informática* o de procesamiento de datos personales-nominativos; que deja de lado el enfoque individualista o negativo con que fue concebido para plantearse desde una perspectiva socializadora y positiva (ya no es el "derecho a ser dejado a solas")."[38]

Dentro de la historia legislativa de este derecho, es importante hacer mención de la gran cantidad de leyes y reglamentos tanto internos como externos respecto a la protección sobre el manejo y transmisión de los datos personales, los cuales, evidentemente, forman parte de la esfera íntima de la vida privada de las personas. Esta gran ola legislativa responde a la constante amenaza que ha sufrido la vida íntima , producto de un verdadero contrabando de información del cual somos víctimas casi todos. De esta manera queda claro que proteger la intimidad del ser humano no es más un asunto propiamente constitucional, ya que el amparo que las Cartas Fundamentales otorgan frente a este derecho debe verse respaldado por la dictación de leyes, decretos, reglamentos y acuerdos internacionales, en constante proceso de evolución y perfeccionamiento alrededor de todo el mundo.

Como consecuencia de ello, el concepto de lo que debe entenderse por derecho a la vida privada también ha sufrido algunas modificaciones, tema que será tratado a continuación.

---

[37] Citado por Mercedes URIOSTE, Protección de datos personales, pág. 50 de texto publicado en http://comunidad.derecho.org/redi/Habeas6.zip, visitada en enero de 2002.

[38] Renato JIJENA LEIVA, La nueva ley chilena de protección de datos personales, N°19.628 del 28 de agosto de 1999, pág. 5, informe legal, 1999.

Evolución Conceptual del Derecho a la Vida Privada

Conceptos jurídicos tradicionales: ¿ intimidad, privacidad o vida privada?

Tanto dentro de la doctrina como dentro de la legislación y la jurisprudencia, los términos "*vida privada*", "*intimidad*" o "*privacidad*" se han utilizado y se utilizan para referirse a aquella parte de nuestras vidas que no debe ser revelada a los demás. Al respecto han existido gran cantidad de debates sobre si se trata de términos que pueden considerarse como análogos, o si en realidad existen diferencias importantes entre ellos. A modo de introducción, debe mencionarse uno de los debates más interesantes, desde mi punto de vista, y de mayor relevancia dentro de la doctrina chilena que se produjo en el seno de la Comisión de Estudio de la Nueva Constitución sobre este tema.

En la sesión 129, celebrada el 12 de junio de 1975, el señor Guzmán manifestaría que *"la intimidad es todavía una zona más profunda y sensible que la privacidad. Es algo todavía más sutil y, por lo tanto, de menor alcance en su extensión".*[39]De esto se desprendería que entre las palabras privacidad e intimidad hay una diferencia de fondo en cuanto la primera representaría el género y la segunda la especie. El señor Ovalle, por su parte, manifestaría *que "es más conveniente la expresión "vida privada" en vez de la palabra "privacidad", porque el concepto de vida privada está más desarrollado en el lenguaje común. Ya hay una especie de reconocimiento en la colectividad de que lo que se respeta es la vida privada. No es la vida hacia el exterior; es la vida interna, dentro del hogar; y la privacidad es un término menos usado, menos conocido. En cambio, la forma "vida privada" constituye una referencia más permanente". A esto, el señor Guzmán respondió que "Tocante a la expresión "vida privada" y al término "privacidad", manifiesta que se inclina por este último porque designa un valor, mientras que aquella expresión designa solamente una realidad de hecho. La persona tiene derecho a la vida privada, pero también tiene derecho a que esa vida privada permanezca como tal. Y ése es el valor que se ha llamado "privacidad", el cual va más allá del hecho de la vida privada. (...)Decir "protección a la vida privada" podría prestarse a dudas respecto de si lo que se está protegiendo es el derecho a que una persona tenga vida privada. Queda más claro y es más fuerte decir "privacidad", porque significa que esa vida privada debe permanecer como tal".*[40] Sin embargo, en la Constitución de 1980 el término que se adoptó fue el de vida privada, ya que, como lo manifestara el señor Ovalle, la palabra "privacidad" no existía en ese entonces en el diccionario de la Real Academia.

No nos ha sido indiferente el averiguar si estos términos son jurídicamente sinónimos o si en realidad, es posible que dentro de ellos existan ciertas diferencias. Por consiguiente, procederé a analizar cada uno de

[39]Citado por Enrique EVANS DE LA CUADRA en Los Derechos Constitucionales, Tomo I, Editorial Jurídica de Chile, Santiago, 1986, pág. 180.

[40] Ibídem.

ellos, utilizando definiciones, tanto de las leyes, como de la doctrina y la jurisprudencia a nivel nacional como internacional.

El concepto de intimidad:

La palabra "intimidad" tiene su origen en el latín, y deriva del término *intimus*. Dentro del latín existen también expresiones como *amici intimi* (amigos íntimos), o *intimus consillis eorum* (confidentes de sus secretos). De ello se desprende que el significado de esta palabra haga alusión a lo íntimo, secreto, recóndito, profundo, propio.[41]

Es curioso que la palabra "intimidad" no solamente sea utilizada en los países de habla hispana. Si revisamos otros idiomas, veremos que también se encuentra incorporada en otras lenguas.

En alemán: intimität.
En francés: intimité.
En italiano: intimitá.[42]
En inglés: intimity.
En español: intimidad.

Es necesario dejar en claro que en inglés, la palabra *intimity* se suele emplear para denominar las relaciones sexuales ilícitas, por lo que se ha evitado utilizarla para el objeto a que nos referimos aquí, quedando sólo la palabra privacy para designar tanto a la intimidad como a la vida privada.

De acuerdo al Diccionario de la Real Academia Española, *intimidad* se define como "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia"[43]. Sin embrago, el significado axiológico se torna insuficiente, por lo cual debemos recurrir a su significado jurídico. Dentro de la doctrina y la jurisprudencia, innumerables son las definiciones que se le atribuyen a esta palabra.

Adriano de Cupis entiende por intimidad a "la necesidad consistente en la exigencia de aislamiento moral, de no comunicación externa, de cuanto concierne a la persona individual".[44]

---

[41] Ver también a Raúl GARCÍA ASPILLAGA, La vida privada y la intimidad de las personas, Tesis de Grado de la Facultad de Derecho de la Pontificia Universidad Católica de Chile,1988, pág. 49.

[42] Incluso en italiano se utiliza la palabra "riservatezza". Algunos juristas italianos como F. Bricola hablan del "diritto alla riservatezza", haciendo una distinción entre estos dos términos.

[43] Diccionario de la Lengua Española, Real Academia Española, Vigésima Primera Edición, Madrid, 1992,pág. 835.
[44] Citado por Raúl GARCÍA ASPILLAGA, La vida privada y la intimidad de las personas, Tesis de Grado de la Facultad de Derecho de la Pontificia Universidad Católica de Chile,1988, pág. 123.

Por su parte, Miguel Bajo Fernández la considera como "ese ámbito personal donde cada uno, preservado del mundo exterior, encuentra las posibilidades de desarrollo y fomento de su personalidad. Se trata pues, de un ámbito personal reservado a la curiosidad pública, absolutamente necesario para el desarrollo humano y donde enraíza la personalidad".[45]

Fried, en un trabajo de 1979 que lleva por título *An anatomy of value* define a la intimidad como "control sobre la información que nos concierne".[46]

R. Nerson la define por su parte como "un sector personal reservado a fin de hacer inaccesible al público, sin la voluntad del interesado, eso que constituye lo esencial de la personalidad". [47]

Es prudente en todo caso hacer una distinción entre *intimidad* y *derecho a la intimidad*. Mientras que el primer concepto hace alusión a una parte de la esfera de la vida de las personas, soy de la idea de que es más adecuado hablar del "derecho a la intimidad", ya que comprende la protección jurídica que el concepto trae consigo. Este último también ha sido ampliamente definido por la doctrina, como veremos a continuación.

En 1873, el juez T. Cooley se había referido someramente al derecho a la intimidad como "el derecho a ser dejado tranquilo y de no ser arrastrado a la publicidad". Warren y Brandeis, a pesar de definir al derecho a la intimidad como el "derecho a ser dejado a solas, a ser dejado en paz", en su obra *El derecho a la Intimidad* han optado por determinar las limitaciones que este derecho comprende, haciendo una sustanciosa enumeración de situaciones, que según los autores, no atentan contra la intimidad.[48]

Manuel Abdalejo lo considera como " aquel del que es titular un sujeto de derecho, que lo faculta, en primer lugar, para decidir libremente que circunstancias o pensamientos quedan excluidos del conocimiento ajeno, y en segundo lugar controlar aquellos que conocidos no lo son en respecto a su persona". De esta definición, según Tomás Vial Solar, se desprenden dos aspectos de la vida íntima de las personas, en sus vertientes activa y pasiva.[49]

---

[45] Ibídem, pág. 124.

[46]Citado por José CUERVO, La intimidad informática del trabajador, pág 4, de texto publicado en http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=106971, visitada en diciembre de 2001.

[47] Citado por Eduardo NOVOA MONREAL, Derecho a la vida privada y Libertad de Información, Siglo XXI Editores SA de CV, México D.F., cuarta edición, 1989, pág. 31, nota 30.

[48] Samuel WARREN y Louis BRANDEIS, El Derecho a la Intimidad, Editorial Civitas, Madrid, 1995, págs. 21, y 61 y siguientes.

[49] Tomás VIAL SOLAR, citando a Manuel ABDALEJO en El derecho a la vida privada y a la libertad de expresión en las constituciones de Chile y España: una propuesta de criterios de análisis, Tesis para optar al grado de Magíster en derecho público de la Facultad de Derecho de la Pontificia Universidad Católica de Chile,1997, pág. 94, nota 11.

Para Georgina Battle Sales, se trata de "el derecho que compete a toda persona a tener una esfera reservada en la cual desenvolver su vida, sin que la indiscreción ajena tenga acceso a ella. Es, en definitiva, el derecho que concierne a la persona de ser ella la que determine cuando y hasta donde entrar en contacto con la soledad".[50]

Julio Núñez Ponce, jurista peruano, define por su parte al derecho a la intimidad como "el derecho que compete a toda persona a tener una esfera reservada en la cual desenvolver su vida sin que la indiscreción ajena tenga acceso a ella".[51]

La Enciclopedia Omeba define al derecho a la intimidad como "un derecho absoluto de cada persona, a que los otros no intervengan en su vida, dañándole, incomodándole o afligiéndole. Toda persona tiene derecho a exigir que sus asuntos particulares no sean comentados o escudriñados en público, sin su consentimiento".[52]

La Conferencia Nórdica, celebrada en Estocolmo en mayo del año de 1967, procedió a definir a la vida privada como "el derecho a vivir en una forma independiente de su propia vida, con un mínimo de injerencia ajena".[53] Junto con esta breve definición, en aquella conferencia también se procedió a hacer una enumeración de las diferentes formas de que representan atentados al derecho a la intimidad.

Luis García San Miguel parece ser más práctico. Nos indica que "definamos como definamos la intimidad, casi todos admitirán que este derecho tiene que ver con la posibilidad de que algo de lo que hacemos o lo que somos (sean cuales sean los confines de ese algo) no sea conocido por los demás y, si fuera conocido por algunos, éstos no lo den a conocer a otros." [54]

El concepto de privacidad:

La palabra "privacidad" ha sido muy usada tanto a nivel doctrinario, como legislativo e incluso jurisprudencial. Tiene su origen en la palabra *privatus*, que viene del latín y que significa privado, particular, propio, personal, individual, idioma del cual también se desprende la expresión *in privatus*, que significa en privado, a solas.[55] El término *privacy*, que en inglés significa "The right to be let alone; the right of a person

---

[50] Citado por Raúl GARCÍA ASPILLAGA, La vida privada y la intimidad de las personas, Tesis de Grado de la Facultad de Derecho de la Pontificia Universidad Católica de Chile,1988, pág. 123, nota 8.
[51] Julio NÚÑEZ PONCE, La acción constitucional de Habeas Data y la comercialización de información judicial, en pág. 4 de texto publicado en http://vlex.com/redi/No._38_-_Septiembre_del_2001/14, visitada en enero de 2002.

[52] Enciclopedia Jurídica Omeba, Tomo XVI. Editorial Bibliográfica Argentina, S.R.L., Buenos Aires, 1962.

[53] Citado por Eduardo NOVOA MONREAL, Derecho a la vida privada y Libertad de Información, Siglo XXI Editores SA de CV, México D.F., cuarta edición, 1989, pág 33.

[54] Citado por José CUERVO, La intimidad informática del trabajador, pág 4, de texto publicado en http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=106971, visitada en diciembre de 2001.

[55] Rodrigo BORJA CEVALLOS, Enciclopedia de la Política, pág. 784, Fondo de la Cultura Económica, México D.F., 1997, primera edición.

to be free from unwarranted publicity. Term "right of privacy" is generic term encompassing various rights recognized to be inherent in concept of ordered liberty, and such right prevents governmental interference in intimate personal relationship or activities, freedoms of individual to make fundamental choices involving himself, his family, and his relationship whit others"[56]. Este es el término que la doctrina de habla inglesa más utiliza para referirse a la vida privada de las personas. El anglicismo "privacidad" no se encontraba en el idioma castellano, pues el Diccionario de la Lengua de la Real Academia Española no lo definía. Sin embargo, en la página de Internet de Real Academia, curiosamente esta palabra se encuentra ya incorporada, y se define como "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión".[57] También se define la palabra "privado", que en sus diferentes acepciones significa "que se ejecute a vista de pocos, familiar o domésticamente, sin formalidad ni ceremonia alguna" y "particular y personal de cada uno".[58]

Según David Casacuberta, la obra de Alan F. Westin (1967) es uno de los textos claves para hablar de privacidad. Allí se define nuestro sujeto de estudio de la forma siguiente: "El derecho de los individuos, grupos o instituciones a determinar por sí mismos, cuando, cómo y hasta qué punto se puede comunicar a terceras personas información referida a ellos".[59] En opinión personal del autor, los medios pueden haber cambiado mucho desde 1967, pero la definición sigue siendo excelente.

Complementando la definición de Westin, es interesante mencionar las cuatro situaciones básicas que, según este autor, deben desprenderse de este concepto:

1) Soledad.- de orden físico, excluye cualquier contacto material; es el último estado de la "privacy".
2) "Intimidad" (intimacy).- sin aislamiento, que se circunscribe a un ámbito de relaciones restringidas. Se define porque el individuo actúa como parte de una pequeña unidad que reclama y está preparada para ejercer una segregación corporativa que permite alcanzar una relación franca, relajada y cerrada entre dos o más individuos.
3) Anonimato.- que implica la falta de identificación, pero que se produce dentro del grupo.
4) Reserva.- el estado más sutil de la intimidad, que supone la erección de una barrera psicológica frente a intromisiones. [60]

---

[56] Definición obtenida del BLACK'S LAW DICTIONARY, Fifht Edition By The Publisher's Editorial Staff, St. Paul Minn, West Publishing CO, 1979, pág. 1075.
[57] Definición obtenida de la página electrónica de la Real Academia Española, cuya dirección es www.rae.es, visitada en abril de 2002.

[58] Diccionario de la Lengua Española, Real Academia Española, Vigésima Primera Edición, Madrid, 1992,pág. 1183.

[59] David CASACUBERTA citando a Alan F. WESTIN en La privacidad en los nuevos medios electrónicos. ,publicado en http://v2.vlex.com/global/redi/redi_numero.asp?numero=%2311&fecha=Junio+1999, pág. 1, visitada en diciembre de 2001.

[60] Citado por José CUERVO, La intimidad informática del trabajador, pág 3, de texto publicado en http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=106971, visitada en diciembre de 2001.

Para Lusky, la privacidad o *privacy* "más que un mero sentido estático de la defensa de la vida privada del conocimiento ajeno, tienen una función dinámica de posibilidad de controlar la circulación de informaciones relevantes para cada sujeto".[61]

Según Parker, en otro trabajo de 1974, con el título *A Definition of Privacy*, la define como "control sobre cuándo y quién puede percibir diferentes aspectos de nuestra persona".[62]

Davara Rodríguez define a la privacidad como "término al que podemos hacer referencia bajo la óptica de la pertenencia de los datos a una persona -su titular- y que en ellos se pueden analizar aspectos que individualmente no tienen mayor trascendencia, pero que al unirlos a otros pueden configurar un perfil determinado sobre una o varias características del individuo que éste tiene derecho a exigir que permanezcan en su esfera interna, en su ámbito de privacidad". [63]

La privacidad es entendida, según Herrera Bravo como "la información personal confidencial, desarrollada en un espacio privado la que no debe ser expuesta a terceros, pues su conocimiento podría ocasionar un manejo de la información que no es deseado o que incluso es motivo de rechazo por la persona".[64]

Hernán Corral Talciani se ha referido a la privacidad como bien jurídico así: "es la posición de una persona (o entidad colectiva personal) en virtud de la cual se encuentra libre de intromisiones o difusiones cognoscitivas de hechos que pertenecen a su interioridad corporal y psicológica o a las relaciones que ella mantiene o ha mantenido con otros, por parte de agentes externos que, sobre la base de una valoración media razonable, son ajenos al contenido y finalidad de dicha interioridad o relaciones". [65]

Concepto de vida privada:

El concepto de "vida privada" ha sido también muy utilizado por parte de los estudiosos de este tema. Su uso ha tenido gran aceptación incluso en distintos idiomas.

En alemán: privat leben.

En francés: vie privée.

---

[61] Citado por María Carolina ORTÚZAR VILLAROEL, El nuevo concepto de Derecho a la Intimidad y su protección en la era tecnológica, Tesis de grado de la Escuela de Derecho de la Universidad Católica de Valparaíso, 1996, pág. 27.

[62] Citado por José CUERVO, La intimidad informática del trabajador, pág 3, de texto publicado en http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=106971, visitada en diciembre de 2001..

[63] Ibídem, pag 3.

[64] Rodolfo HERRERA BRAVO, Chile: ¿Por qué la Protección de Datos Personales es una garantía básica de los Derechos fundamentales?, en Revista Electrónica de Derecho Informático N° 38 de septiembre de 2001,pág. 4, cuyo texto se encuentra en http://vlex.com/redi/No._38_-_Septiembre_del_2001/14

[65] Hernán CORRAL TALCIANI, Configuración Jurídica del Derecho a la Privacidad II, de texto publicado en Revista Chilena de Derecho, Vol. 27 N°2, pág. 347, Sección Estudios.

En inglés: private life.
En español: vida privada.

Este concepto, partiendo de la definición de *privada* que da el Diccionario de la Lengua Española, podría definirse como "aquella parte de la vida humana que se desarrolla a la vista de pocos o que constituye la vida personal y particular"[66]. Definitivamente, sin tener un alcance puramente jurídico, la definición no es mala, ya que abarca las facultades de desarrollarse en privado e incluso de ser dejado en paz.

Someramente, en el anteproyecto de Reforma de la Ley 18.313, se dejó constancia de que "se considerarán en todo caso pertenecientes a la vida privada en los hecho relativos a la vida sexual, conyugal y doméstica de una persona, salvo que ellos consistieren en delitos de acción pública y hubieren sido cometidos con grave escándalo".

Dentro de la doctrina chilena, Eduardo Novoa Monreal considera que la vida privada "está constituida por aquellos fenómenos, comportamientos, datos y situaciones de una persona que normalmente están sustraídos al conocimiento de extraños y cuyo conocimiento por éstos puede turbarla moralmente por afectar su pudor a su recato, a menos que esa misma persona asienta a ese conocimiento". [67]

Enrique Evans de la Cuadra piensa que "el concepto de "vidas privada"está directamente vinculado al de "intimidad", a ese ámbito en que el ser humano y la gente de sus afectos conviven, conversan, se aman, planifican el presente y el futuro, comparten alegrías y tristezas, gozan del esparcimiento, incrementan sus virtudes y soportan y superan sus defectos, y fomentan sus potencialidades humanas para su progreso integra, todo ello sin la intervención o presencia de terceros".[68]

Las Pautas Éticas para los Medios de Comunicación, adoptadas por el Consejo de Ética de los Medios de Comunicación Social de Chile entiende a la vida privada como "las conductas, el espacio, que cada persona necesita y desea mantener alejados de los ojos y oídos extraños. Se trata del núcleo personal, del recinto de expansión y verdadera libertad del sujeto, que éste no acepta compartir con nadie o que comparte con sus íntimos". [69]

---

[66] Diccionario de la Lengua Española, Real Academia Española, Vigésima Primera Edición, Madrid, 1992,pág. 1183.

[67] Eduardo NOVOA MONREAL, Derecho a la vida privada y Libertad de Información, Siglo XXI Editores SA de CV, México D.F., cuarta edición, 1989, pág 49.

[68] Enrique EVANS DE LA CUADRA, Los Derechos Constitucionales, Tomo I, Editorial Jurídica de Chile, Santiago, 1986, pág. 172.

[69] Citado por Miguel Ángel FERNÁNDEZ, refiriéndose al Dictamen N°55, pronunciado el 25 de junio de 1997, reproducido en Consejo de Ética de los Medios de Comunicación: Fallos 1997, en Libertad de expresión, censura previa y protección, en Revista Chilena de Derecho, Vol. 28, año 2001, pág. 398.

El profesor José Luis Cea Egaña la define como "intrusión maliciosa en asuntos, documentos, comunicaciones, o recintos que el titular del bien jurídico protegido no desea que sean conocidos por terceros sin su consentimiento previo". [70]

Así mismo, la Revista de Derecho y Jurisprudencia de Chile, en su Tomo XC, número 2 del año 1993 en su sección quinta, define a la vida privada como "aquella zona que el titular del derecho no quiere que sea conocida por terceros sin su consentimiento".

Raúl García Aspillaga define por su parte a la vida privada como "el ámbito de la personalidad de todo individuo constituido por aquellos fenómenos, actuaciones, situaciones, estados, etc... relativos a la propia persona y a sus vínculos afectivos más cercanos, que usualmente están sustraídos al conocimiento, contacto, presencia o intervención de extraños, ya que de lo contrario redundaría en un estado de alteración del sujeto al ver afectado su pudor o recato, por una parte, o, por otra, su anhelo de soledad y reconocimiento, todo lo cual sin perjuicio de que el interesado consienta en que se tome conocimiento de su realidad íntima o esté llano a permitir la intervención de terceros en sus espacios y momentos de paz".[71]

Para el francés Gérard Lyon-Caen, la vida privada comprende "las circunstancias de la vida familiar (esponsales, matrimonios, divorcio), también la vida amorosa; las circunstancias de la vida profesional".[72]

Lucien Martín diría que "la vida privada es la vida familiar, personal del hombre, su vida interior, espiritual, la que lleva cuando vive detrás de su puerta cerrada".[73]

Pero, como lo señalaba anteriormente, soy partidario de que es más adecuado referirse al concepto de *derecho a la vida privada*, antes que a la *vida privada* simplemente, ya que son definitivamente dos conceptos distintos, a los cuales muchas veces se confunde, y no es posible considerar que la protección jurídica merece el mismo ámbito de interpretación del concepto que ella ampara. Revisemos las definiciones que tanto la legislación como la doctrina han dado al concepto de "derecho a la vida privada".

La Asamblea Constitutiva del Consejo de Europa, celebrada en 1970, considera de una manera sumamente amplia, y desde mi punto de vista bastante completa al derecho a la vida privada, diciendo que ella "consiste esencialmente en poder conducir su vida como se la entiende, con un mínimo de injerencia. Él concierne a la vida privada, a la vida familiar y a la vida del hogar, a la integridad física y moral, al honor y a la reputación,

---

[70] José Luis CEA EGAÑA, Manual de Derecho Constitucional, Tomo II, pág. 92.

[71] Raúl GARCÍA ASPILLAGA, La vida privada y la intimidad de las personas, Tesis de Grado de la Facultad de Derecho de la Pontificia Universidad Católica de Chile,1988, págs. 166 y 167.

[72] Citado por Tomás VIAL SOLAR, El derecho a la vida privada y a la libertad de expresión en las constituciones de Chile y España: una propuesta de criterios de análisis, Tesis para optar al grado de Magíster en derecho público de la Facultad de Derecho de la Pontificia Universidad Católica de Chile,1997, pág. 93, nota 8.

[73] Lucien MARTÍN, Le secret de la vie privée, Revue Trimestrelle de Droit Civil, LVII, T.57, an 1959, pág. 230

al hecho de no ser presentado bajo una falsa apariencia, a la no divulgación de hechos inútiles o embarazosos, a la publicación sin autorización de fotografías privadas, a la protección contra el espionaje y las indiscreciones injustificables o inadmisibles, a la protección contra la utilización abusiva de las comunicaciones privadas, o la protección contra la divulgación de informaciones comunicadas o recibidas confidencialmente por un particular; sin que puedan prevalerse del derecho de protección a su vida privada las personas que por sus propias actividades han alentado las indiscreciones de las cuales se van a quejar posteriormente". [74]

William F. Swinder lo considera como "el derecho a vivir su propia vida en soledad sin estar sometido a una publicidad que no se ha provocado ni deseado. En resumen, es el derecho a ser dejado solo. Existen, sin embargo, momentos en que el individuo lo quiere o no, se ve forzado a intervenir en un dominio de interés general o público, Cuando tal caso sucede, el individuo sale de su retiro y ya no es una intrusión en su vida privada publicar por ejemplo su foto acompañada de una explicación de los hechos".[75]

La *Office of Science and Technology of the Executive Office of the President*, celebrada en 1967 diría que "el derecho a la vida privada es el derecho del individuo de decidir por sí mismo en qué medida compartirá con otros sus pensamientos, sus sentimientos y los hechos de su vida privada. En realidad, lo que es privado varía según los días y las circunstancias".[76]

El debate respecto de cuál de los términos empleados es el correcto todavía persiste. Efectivamente, los tres conceptos son ampliamente usados tanto por la legislación, como por la doctrina y la jurisprudencia. Como primera aproximación, quiero insistir en que no es lo mismo hablar, como ya lo manifestaba anteriormente, de *intimidad, privacidad o vida privada* que de *derecho a la intimidad, derecho a la privacidad o derecho a la vida privada*. Mientras que las primeras acepciones tienen relación con aquella parte de la vida de las personas considerada como especialmente propia o íntima, las segundas son el amparo o la protección jurídica que el sistema normativo entrega a las primeras. De lo anterior se desprende que efectivamente, antes de buscar el resguardo legal de aquella parte tan delicada de nuestras vidas, es prudente delimitarla en busca de un mejor amparo o una mejor protección frente a posibles amenazas o violaciones que pueda sufrir. Lamentablemente, todavía muchos confunden estos dos conceptos.

Hay también quienes se refieren a *la protección del derecho a la vida privada*, concepto que también es distinto a los dos anteriores, pues representa el amparo a un reconocimiento jurídico, cual es un derecho, el que a su vez resguarda una garantía, en este caso, la vida privada de las personas. Por lo que acabo de

---

[74] Citado por Eduardo NOVOA MONREAL, Derecho a la vida privada y Libertad de Información, Siglo XXI Editores SA de CV, México D.F., cuarta edición, 1989, pág. 34.

[75] Citado por Raúl GARCÍA ASPILLAGA, La vida privada y la intimidad de las personas, Tesis de Grado de la Facultad de Derecho de la Pontificia Universidad Católica de Chile,1988, pág. 121.

[76] Ibídem, pág. 124.

explicar, cada una de estas tres expresiones debería ser utilizada de acuerdo a la idea que se quiere manifestar, y evitar en lo posible aplicarse como sinónimos.

Poco se ha hablado en cambio del "derecho a la reserva", que en palabras de P. Rescigno comprende "la pretensión del individuo de ver impedida la curiosidad de otros, prohibiéndose la indiscreción y la publicidad no querida, el conocimiento y la divulgación de las vicisitudes personales y familiares". Según Novoa Monreal, tal definición es criticada porque tiene un alcance puramente subjetivo.[77]

En cuanto al significado propiamente tal de las palabras *intimidad*, *privacidad* y *vida privada*, para cierta parte de la doctrina, entre ellos el chileno Renato Jijena Leiva, serían sinónimos, partiendo de la base que de ello no se desprende ningún efecto jurídico.[78]

Dentro de la doctrina internacional, el español González Gaitano, al tratar de la localización de la palabra intimidad, señala que "así como la vida pública y la vida privada en términos relativos uno del otro, intimidad es un término absoluto. La vida privada se define por relación a la vida pública y viceversa. Esa relación es variable en cada cultura y según los momentos históricos la intimidad está al margen de la dialéctica público-privado, pero a la vez está en la raíz de la posibilidad de las dos esferas y de su mutua dependencia. Sólo desde la intimidad puede haber vida privada y vida pública y sólo desde el reconocimiento y protección de su valor absoluto pueden definirse los ámbitos de las otras dos esferas".[79]

Soy de la postura de que entre los términos antes expuestos, es más adecuado ocupar la expresión "derecho a la vida privada", porque desde mi punto de vista, al ser un concepto de amplia interpretación, abarca dentro de él los términos "intimidad" y "privacidad". Respecto de este último, no soy partidario de que se lo ocupe con tanta amplitud ya que al ser un anglicismo, su traducción muchas veces no es tan íntegra como se quisiera.

Es curioso que incluso algunos autores hablen de la "intimidad de la vida privada", justamente como si entre estos dos conceptos nuevamente el primero fuera la especie y el segundo el género. Esta expresión fue en 1890 muy utilizada por los norteamericanos Warren y Brandeis, y en la actualidad, dentro de la doctrina francesa, autores como Pierre Kaiser y Henri Mazeaud la utilizan con mucha frecuencia.

---

[77]Eduardo NOVOA MONREAL, Derecho a la vida privada y Libertad de Información, Siglo XXI Editores SA de CV, México D.F., cuarta edición, 1989, pág. 32.

[78] Incluso JIJENA LEIVA utiliza la palabra *privacy*, pero en lo personal no estoy de acuerdo con emplearla porque referirse a ella es referirse a una parte determinada de la vida privada de las personas y no al concepto genérico, además que no es lo más adecuado traducirla al español como privacidad.

[79]Citado por José CUERVO, La intimidad informática del trabajador, pág 3, de texto publicado en http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=106971, visitada en diciembre de 2001.

Dentro de la doctrina alemana, la cual será analizada con más detalle más adelante, la distinción entre los términos antes aludidos también ha encontrado cabida, de tal suerte que de ellos se desprenden *gradaciones* dentro de la vida privada y sus aspectos.[80]

En cuanto a las definiciones propiamente tales de estos tres conceptos, soy de los que cree que no existe una definición perfecta ni menos un acuerdo unánime dentro de la doctrina, ya que el contenido y los elementos de lo que debe entenderse como vida privada son absolutamente variables según diversos factores. Este criterio ha sido ya enunciado anteriormente por el American Law Insitute, que ha sostenido, refiriéndose al contenido de la vida privada que "no hay una demarcación bien nítida entre lo que debería y no debería estar permitido". Por su parte, la Comisión Internacional de Juristas diría que "la vida privada es algo difícil de definir por tratarse de algo esencialmente subjetivo".[81]

Como lo indica Ángela Vivanco, "de tal diversidad de conceptos y de campos abarcados, es fácil deducir que la vida privada es un concepto eminentemente social, que por ende varía culturalmente, y que depende mucho de la época en que se vive, de las tradiciones de un pueblo y de los elementos religiosos y morales que se encuentren comprometidos en ese punto".[82]

Hay autores como Eduardo Novoa Monreal y Raúl García Aspillaga que han optado por hacer una enumeración de los aspectos que deben considerarse dentro de la vida privada de las personas. Pero, sin pretender descalificar una enumeración que sin duda es valiosa, como se explicaba anteriormente, y por tratarse de un concepto puramente evolutivo, su aplicación se vería limitada por diversos hechos. Hago alusión, a modo de ejemplo a variantes como la época, la cultura, la moral, la religión, el rol que la persona desempeña en la sociedad, e incluso los medios a través de los cuales se invade la vida privada de las personas, como es el caso de medios electrónicos como Internet. Refiriéndose a esto último, el español David Casacuberta manifiesta que "si bien los nuevos medios electrónicos no han modificado el concepto del derecho a la privacidad sí que han modificado las formas en que éste puede ser protegido o puesto en peligro". [83]

Por todo lo anteriormente expuesto, pienso que puede ser interesante abarcar dentro de una definición justamente factores que siempre irán cambiando, con la intención de que éstos se adapten a la época y al lugar donde requieren una interpretación. Desde este punto de vista, podría definirse al derecho a la vida privada

[80] Ver a este respecto la obra de Eduardo NOVOA MONREAL, Derecho a la vida privada y Libertad de Información, Siglo XXI Editores SA de CV, México D.F., cuarta edición, 1989, pág. 47.

[81] Ibídem, pag 34.

[82] Ángela VIVANCO, Las libertades de Opinión y de Información, Editorial Andrés Bello, Santiago, 1992, pág. 219.

[83]David CASACUBERTA, La privacidad en los nuevos medios electrónicos. Aspectos éticos y sociales, en texto publicado en http://v2.vlex.com/global/redi/redi_numero.asp?numero=%2311&fecha=Junio+1999, visitado en enero de 2002.

como **el derecho que tiene toda persona para que, de conformidad con la época, la sociedad, la cultura, el rol que la persona tiene en el ambiente en que se desenvuelve, su origen, su edad, su estrato social y su desarrollo físico psíquico y espiritual, aquellos datos que formen parte de la esfera de su vida íntima no sean divulgados sin su consentimiento a terceros, ni sea perturbado su derecho a ser dejado a solas, a menos que existan intereses legítimos para ello.**

La definición recién propuesta merece las siguientes acotaciones: a) soy de la idea de que estamos frente a un concepto que, como bien lo indicaba ya la Comisión Internacional de Juristas, es subjetivo en el sentido de que corresponde a cada individuo "autodeterminar" los márgenes dentro de los cuales se delimita su esfera íntima, dentro de criterios medianamente racionales; b) está en manos del juez el determinar todos los factores que forman parte de la definición antes mencionada, en conformidad de cada persona, buscando justamente que éstos no caigan en absurdos; c) para evitar que la apreciación del juez se torne personal y subjetiva, éste debe regirse por las normas que la Constitución y las leyes han consagrado respecto de los demás derechos esenciales del hombre, fundados éstos básicamente sobre la dignidad del ser; d) el derecho a la vida privada de las personas evoluciona a lo largo de la existencia de cada ser humano, y por consiguiente, no será lo mismo la esfera íntima que tiene un niño, un adolescente o un adulto; e) creo sin duda que está en manos de la jurisprudencia de alguna manera trazar los márgenes dentro de los cuales éste concepto debe ser entendido, abierto por supuesto a que ésta, de conformidad con el tiempo, pueda perfeccionarse en consideración de la época y de las circunstancias. Recordemos que en la Comisión de Estudio de la Nueva Constitución ya se reconocía a la jurisprudencia como medio para definir y delimitar el alcance que debía tener el derecho a la vida privada de las personas.[84]

En esta propuesta pretendo demostrar que el derecho a la vida privada es evolutivo también para cada individuo, pues el marco que abarca la vida privada de un ser humano perfectamente puede variar según su edad y según la sociedad en que se encuentra. No en vano he querido dejar al contenido propiamente tal de la vida privada, vale decir "su esfera íntima" y "su derecho a ser dejado a solas" de una manera bastante difusa y amplia, pues como bien lo indica el autor chileno Renato Jijena Leiva, "ello representaría una ventaja, pues permitiría una constante evolución y adaptación del concepto". [85]

A pesar de existir diferentes teorías para explicar el concepto de vida privada, merece desde mi punto de vista especial atención la *Teoría de las* Esferas, proveniente de la doctrina alemana. Según esta postura, la vida privada de las personas está conformada por tres esferas. La primera de ellas es la "esfera íntima", en alemán *privatsphäre*, la cual abarca todos aquellos comportamientos, noticias o discursos que el sujeto pretende que no sean revelados al público. Aquí debe incluirse también su imagen física y su comportamiento aún fuera de

[84] En la Sesión celebrada por la Comisión de Estudio de la Nueva Constitución con fecha 12 de junio de 1975 se señalaba que : *"En cuanto se fije por la jurisprudencia los límites, le parece que va a ser inevitable que así sea"*, de palabras pronunciadas por don Jaime Guzmán Errázuriz, refiriéndose al alcance que debe tener el ámbito de la vida privada de las personas.

[85] Renato JIJENA LEIVA, Chile, la protección penal de la intimidad y el delito informático, Editorial Jurídica de Chile, Santiago, 1992, pág. 41.

su domicilio, que no deben ser conocidos sino por aquellos que se hallan en contacto con él. En segundo lugar está la "esfera confidencial", en alemán *vertrauensphära*, la cual dentro de un cuadro de cobertura menor comprende lo que el sujeto hace partícipe a otra persona de confianza. De esta esfera quedan excluidas, aparte del público en general, aquellas personas que operan en la vida privada y familiar. Dentro de esta esfera se incluye la correspondencia, memorias, diarios de vida, etc... La última esfera, obviamente cada vez con un radio más limitado, se conoce como la "esfera del secreto", en alemán *geheimsphäre*, la cual comprende las noticias y hechos que por su carácter extremadamente secreto, hará que éste sea inaccesible a todas las demás personas.[86]

Nuevos conceptos jurídico derivados de este derecho

Al adentrarse una nueva era en la protección del derecho a la vida privada de las personas, muchos "datos"[87] que a lo mejor hace unos años no tenían relevancia, en la actualidad se han visto como potenciales medios para crear bienes jurídicos de gran cotización en las llamadas sociedades de mercado o sociedades de marketing. Como consecuencia de ello, también nació toda una tendencia destinada precisamente a la *protección de datos.*

Incluso, dentro de la doctrina, autores como F. Hondius han definido a la protección de datos como "aquella parte de la legislación que protege el derecho fundamental de libertad, en particular el derecho individual a la intimidad respecto del procesamiento manual o automático de datos".[88] Otros autores han preferido hablar del "derecho a la protección de datos", cuya traducción al inglés, según Puccinelli es *Data protection* y al alemán *Datenshutz*.

Gran parte de la doctrina ha coincidido en que el derecho a la protección de datos responde a todo un proceso evolutivo del derecho a la vida privada de las personas, reconociéndolo como parte de éste y no como un derecho independiente y autónomo. Olga Estadella Yuste se pronuncia al respecto señalando que "La relación existente entre el derecho a la intimidad y el derecho a la protección de datos personales o a la autodeterminación informativa ha sido analizado de forma diferente por la doctrina. Unos autores han afirmado que los términos "protección de datos" y "protección de la intimidad" son dos nociones diferentes, ya que el interés de proteger la veracidad de los datos y el uso que de ellos se hace no está relacionado necesariamente con la protección de la intimidad individual." Son partidarios de esta postura Cifuentes y Lucas Murillo.

---

[86] Ver También a este respecto la obra de Eduardo NOVOA MONREAL, Derecho a la vida privada y Libertad de Información, Siglo XXI Editores SA de CV, México D.F., cuarta edición, 1989, pág. 4.

[87] Debe entenderse como *dato* al "antecedente necesario para llegar al conocimiento exacto de una cosa o para deducir las consecuencias legítimas de un hecho; representación de una información de manera adecuada para su tratamiento por un ordenador". Diccionario de la Lengua Española, Real Academia Española, Vigésima Primera Edición, Madrid, 1992,pág. 469.

[88] Citado por Oscar PUCCINELLI en El Habeas Data en Indoiberoamérica, pág. 66, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1999.

Algunos han sostenido que el carácter diferenciador de estos términos no reside en su significado, sino que está relacionado con los sistemas legales del *common law* o del *civil law*. Según estos autores, los países de tradición legal de *common law* utilizan más frecuentemente la expresión "protección de la intimidad", mientras que los países de *civil law* utilizan la expresión "protección de datos". [89]Otros autores creen que tal diferenciación es inútil, porque, como lo cita la propia Yustadella Yuste, "data protection is replacing privacy because it indicates a more mundane legal context than that human rights". [90]

En lo personal soy partidario de la postura de Puccinelli, quien a su vez cita a Garzón en el sentido de que la noción de "protección de datos" no es más que una nueva aplicación jurídica del ya conocido derecho a la vida privada de las personas, y que "cuando los individuos consiguen afirmar el derecho a la protección de datos personales, implícitamente se afirma una "parcela" del contenido que comprende el amplio derecho a la intimidad".[91] Veamos en todo caso a continuación las distintas definiciones que la doctrina ha dado a esta nueva rama del derecho a la intimidad.

El derecho a la protección de datos:

El connotado profesor argentino Oscar Puccinelli ha distinguido entre el "derecho *de* la protección de datos" y el "derecho *a* la protección de datos". Se entiende al primero como el "conjunto de normas y principios que, destinados o no a tal fin, y con independencia de su fuente, son utilizados para la tutela de los diversos derechos de las personas –individuales o jurídicas- que pudieran verse afectados por el tratamiento de datos nominativos". Por su parte el derecho *a* la protección de datos sería la "facultad conferida a las personas para actuar *per se* y para exigir la actuación del Estado a fin de tutelar los derechos que pudieran verse afectados por virtud del acceso, registro o transmisión a terceros de los datos nominativos a ella referidos". Es así que el mismo autor explica respecto a sus definiciones que "tanto el derecho *de* la protección de datos como el derecho *a* la protección de datos, en rigor técnico no tienden, como pareciera sugerir su denominación, a la protección de datos en sí, y por lo tanto son conceptos meramente instrumentales, es decir medios para la tutela de otros bienes jurídicos".[92]

Dentro de la doctrina nacional, en el Informe de la Comisión de Constitución, Legislación y Justicia sobre el proyecto para regular la protección de la vida privada se definió al derecho a la protección de datos como "el conjunto de normas jurídicas destinadas a asegurar al individuo el respeto de sus derechos y libertades

[89] Ibídem, pág. 81.

[90] Ibídem, pág. 81.

[91] Ibídem, pág.82.

[92] Ibídem, págs. 65 y 66.

fundamentales y, especialmente, el respeto a su intimidad ante el cada vez más frecuente tratamiento automatizado de los datos de carácter personal".[93]

El derecho a la autodeterminación informativa:

A raíz de la ya comentada sentencia dictada por el Tribunal Constitucional Alemán en el año de 1983, se consolidó este nuevo concepto, *el derecho a la autodeterminación informativa*, de amplia utilización y de gran aceptación en la actualidad por una importante parte de la doctrina. Sin embargo, creo prudente recalcar que no sería esta sentencia la que habría creado esta expresión, ni de hecho ni de nombre.

Según lo indica el profesor alemán Erhard Denninger, la expresión *autodeterminación informativa* se venía fraguando ya desde hace algunos años, y si bien su origen es alemán, salió a la luz a través de sentencias como la de la Ley de ayuda a la inversión de 1954 o la sentencia Lüth de 1958 que se refirió al "valor y la dignidad de la persona que actúa como un miembro libre con autodeterminación libre en una sociedad libre".[94] En cuanto al concepto *derecho a la autodeterminación informativa*, en un informe encargado por Ministerio Federal del Interior alemán del año 1971, Steinmüller y otros hablaban derechamente del "derecho a la autodeterminación informativa sobre la imagen de una persona o de un grupo de personas" o el "derecho a la autodeterminación informativa del ciudadano referente a la imagen de su propia persona". El propio Denninger en 1981 se refiere ya a la "separación de la protección constitucional y el derecho fundamental de autodeterminación informativa". [95]

Pero sin duda alguna que una de las definiciones más celebres de este relativamente nuevo derecho es atribuida al Tribunal Constitucional Federal que a raíz de la ya comentada sentencia de 1983, diría que se trata de "aquel derecho que tiene por objeto garantizar la facultad de las personas para conocer y acceder a las informaciones que les conciernen, archivadas en bancos de datos; controlar su calidad, lo cual implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados, y disponer sobre su transmisión".[96]

---

[93] Cámara de Diputados, Sesión Tercera, celebrada con fecha martes 4 de junio de 1996, pág. 50.

[94] Antonio PÉREZ LUÑO (director de la edición), Problemas actuales de la documentación y la informática jurídica, en capítulo escrito por Erhard DENNINGER, pág. 271, Editorial Tecnos S.A., Madrid, 1987.

[95] Ibídem, pág. 272. Profundiza en esta obra el mismo autor señalando que "Entendiendo el DAI (Derecho a la Autodeterminación Informativa) como facultad general de disponer sobre datos propios personales, el Tribunal ha puesto el acento, de forma decisiva, respecto a una conclusión teórica (y constitucional); la autodeterminación informativa no sólo depende de los datos sino de su elaboración. No es la clasificación abstracta, categórica, de un dato según la mayor o menor cercanía al "ámbito íntimo de la vida" de una persona; tampoco es la cuestión de si un dato por naturaleza tiene caracteres de secreto o no lo que decide si es digno de ser protegido o no, sino el contexto de su uso. La sentencia Zensus parte de la coexistencia de ambos criterios; dice que no depende sólo del tipo de información sino que lo que importa son su utilidad y la posibilidad de su aplicación".

[96] Citado por Antonio PÉREZ LUÑO, Los derechos humanos en la sociedad tecnológica, pág. 140, Editorial CEC, Madrid, 1989.

El concepto de *information control*:

Dentro de la doctrina anglosajona se ha utilizado la expresión *information control*, que en palabras de Westin se refiere al "derecho de los individuos, grupos e instituciones para determinar por sí mismos cuándo, cómo y con qué extensión la información acerca de ellos es comunicada a otros".

Siguiendo los mismo pasos, Freid la ha interpretado como "el control de la información sobre uno mismo, o la habilidad individual de controlar la circulación de la información referente a la persona".[97]

El concepto de libertad informática:

Dentro de la doctrina ha nacido también el concepto de *libertad informática*, que según palabras de Vittorio Frosini se trata de "una nueva forma presentada por el derecho a la libertad personal". [98]

Antonio Pérez Luño nos da una definición más minuciosa ya que según él es un "derecho fundamental de tercera generación que tiene por finalidad garantizar la facultad de las personas de *conocer* y *acceder* a las informaciones que les conciernen, archivadas en bancos de datos; *controlar* su calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados y *disponer* de su transmisión". [99]

El español Pablo Lucas Murillo la entiende como "el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no, para preservar de este modo y en último extremo, la propia identidad, nuestra dignidad y libertad". [100]

Oscar Puccinelli se remite a ella como "aquella proyección del principio -valor- "libertad" que, aplicado a la actividad informática, se traduce en el derecho de los operadores de estos sistemas de colectar, procesar y transmitir toda la información cuyo conocimiento, registro o difusión no esté legalmente restringido por motivos razonables, fundados en la protección de los derechos de las personas o en algún interés colectivo, relevante que justifique tal limitación".[101]

---

[97] Citados por Oscar PUCCINELLI en El Habeas Data en Indoiberoamérica, pág. 66, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1999.

[98] Vittorio FROSINI, Informática y Derecho, pág. 69, Editorial Temis S.A., Santa fe de Bogotá, Colombia, 1988.

[99] Citados por Oscar PUCCINELLI en El Habeas Data en Indoiberoamérica, pág. 67, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1999.

[100] Ibídem, pág. 68.

[101] Ibídem, pág 67.

Resulta interesante preguntarse si los conceptos recién descritos pueden considerarse como sinónimos o si en realidad comprenden aspectos particulares del derecho a la intimidad. Según el ya citado Oscar Puccinelli, refiriéndose a los conceptos antes descritos, ha señalado que "proponemos mantener al "derecho a la protección de datos" como denominación genérica por tener la aptitud mencionada para englobar todas las otras rotulaciones y conceptos –con lo cual el derecho a la autodeterminación informativa bien podría ser una especie de él- , y por haber sido así receptado en las principales normas internacionales sobre la materia, para evitar ambigüedades en el manejo de este vocablo".[102]

El concepto de Habeas Data:

Aún cuando el objetivo de este trabajo no es profundizar en lo que es el habeas data como tal, resulta indispensable considerarlo a la hora de tratar de comprender los medios que las leyes han creado para proteger aspectos de la vida íntima de los seres humanos en estos últimos tiempos. Sin pretender entrar en un estudio detallado del tema, a continuación buscaré el equilibrio para tratar de dar una explicación básica y del todo suficiente.

El concepto *habeas data* significaría a grandes rasgos "traer el dato" (partiendo de la base que mayoritariamente se ha considerado que *habeas corpus* se entiende como "traer el cuerpo"). La palabra *dato* tiene su origen en el latín *datum*, que en definitiva interpretado en este concepto se refiere a informaciones que forman parte de la vida de las personas y que pertenecen a una base o banco de datos[103]. Según palabras de Puccinelli, este concepto "literalmente significa "tenga el dato", y busca asegurar el acceso a informaciones para la tutela de la honra, de la tranquilidad, del patrimonio, de la vida privada, entre diversos valores, contra los atentados efectuados por organismos públicos o de carácter público, en la anotación de datos e informaciones acerca de las personas". [104]

Se dice que el reconocimiento del derecho a controlar los datos de carácter personal tiene su origen el la Constitución de Weimar, del año 1919. En este cuerpo legislativo se reconocía ya el deber de velar por la información que contenían los expedientes personales de los funcionarios públicos. Así lo establecía el mencionado artículo:

"Artículo 129.- Inciso tercero: Todo funcionario debe tener un recurso contra la decisión disciplinaria que le afecte y la posibilidad de un procedimiento de revisión. Los hechos que le son desfavorables no deben ser anotados en su expediente personal sino después de haberle dado ocasión de justificarse respecto a ellos.

El funcionario tiene derecho a examinar su expediente personal.

[102] Ibídem, pág. 69.
[103] Ver la definición de "dato", en nota 87.
[104] Ibídem, pág. 209.

La inviolabilidad de los derechos adquiridos y el recurso a los tribunales para la reclamación de derechos pecuniarios son de modo especial igualmente garantizados a los militares de carrera. Para el resto, su situación está regulada por una ley del Reich (Estado)".[105]

De este artículo se desprenden ya una serie de principios que formarían parte de lo que representa el esquema tradicional del habeas data en la mayoría de los ordenamientos jurídicos: el reconocimiento de un *recurso* para revisar datos de su vida personal, a tener conocimiento de los datos que se guardan sobre su persona, el derecho a un debido proceso, el derecho a que se rectifique la información que se tiene sobre una persona, e incluso el derecho a exigir una indemnización de carácter pecuniario. No son más que las primeras pinceladas de todo un proceso que hasta nuestros días se encuentra en proceso de perfeccionamiento.

En cuanto a la naturaleza jurídica del habeas data, muchos le han atribuido la calidad de derecho: otros hablan de un recurso, de una garantía o de una acción procesal constitucional. Si bien no ha habido un acuerdo unánime por parte de la doctrina, sí puede afirmarse que ello depende de cada legislación.

En la doctrina brasileña, Alfonso Da Silva se refiere al habeas data como "un remedio constitucional, un medio destinado a provocar la actividad jurisdiccional y que, por tal motivo, tiene naturaleza de acción, más específicamente de acción constitucional". [106]

La doctrina argentina cree prácticamente por unanimidad de que se trata de una acción procesal constitucional (Sagües, Bidart, Campos, Quiroga, Lavíe entre otros) mientras que una parte importante de los autores españoles como Pomed Sánchez habla de un derecho personalísimo.[107]

La Corte Constitucional de Colombia se refiere al habeas data como "el derecho autónomo y fundamental que permite a toda persona conocer, actualizar y rectificar las informaciones que sobre ella hayan sido consignadas en bancos de datos y en archivos de entidades públicas o privadas, en defensa de sus derechos fundamentales a la intimidad, a la honra y al buen nombre".

Renato Jijena Leiva dice que: "El *"Habeas Data"* es una acción cautelar de rango constitucional, heredera de otro recurso y tan importante como el *"Habeas Corpus"*, que en las modernas sociedades de la información permite a los titulares de los datos personales o patrimoniales –al decir de una sentencia histórica del Tribunal Constitucional alemán- "autodeterminar" el uso que se haga de sus antecedentes cuando ellos son recopilados, registrados y cruzados computacionalmente". [108]

---

[105] Artículo 129 de la Constitución de Weimar de 1919.

[106] Citado por Oscar PUCCINELLI en El Habeas Data en Indoiberoamérica, pág. 212, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1999.

[107] Ver a este respecto un estudio más minucioso en la ya citada obra de Oscar PUCCINELLI, pág. 212 y siguientes.

[108] Renato JIJENA LEIVA, La nueva ley chilena de protección de datos personales, N° 19.628 del 28 de agosto de 1999, pág. 6, informe legal, 1999.

Resulta interesante mencionar la definición que nos da Marie Claude Mayo, quien utiliza como sinónimos a los conceptos de *habeas data* y *protección de datos personales*, además de su original estilo para definirlo, por lo cual establece que "El *habeas data* o protección de datos personales, establece garantías mínimas de calidad y confiabilidad de los datos nominativos o personales que se recojan; el derecho de las personas a exigir que sus datos personales le sean exhibidos; el derecho a que sean rectificados y el derecho a excluir los datos privados mantenidos sin autorización. Se le grafica de la siguiente forma: Dime qué sabes de mí; dime porqué lo sabes; dime para qué los tienes; si no sabes para qué los tienes, bórralos; si sabes para qué los tienes, dímelo y deja que te lo autorice; si esa información es errónea, déjame rectificarla (...)".[109]

Muchos han asociado al *habeas data* con el *habeas corpus*. Antonio Pérez Luño ha señalado que "Al cotejar el *habeas corpus* y el *habeas data* se comprueba una inicial coincidencia en lo referente a su naturaleza jurídica. En ambos casos no se trata de derechos fundamentales *stricto sensu* , sino de instrumentos o garantías procesales de defensa de los derechos a la libertad personal, en el caso del *habeas corpus*, y de la libertad informática en el caso del *habeas data*." Continúa el español señalando que "El habeas corpus y el habeas data representan, además, dos garantías procesales de aspectos diferentes de la libertad. Así, mientras el primero se circunscribe a la dimensión física y externa de la libertad; el segundo tiende a proteger prioritariamente aspectos internos de la libertad: la identidad de la persona, su autodeterminación, su intimidad (...)".[110]

De lo anteriormente expuesto se puede deducir que el habeas data se ha convertido en la actualidad en una nueva arma para combatir a quienes pretenden atentar contra la vida privada de las personas, especialmente con respecto al manejo de sus datos nominativos. Aún cuando esta acción ha tenido gran aceptación a nivel mundial al habérsele reconocido tanto constitucionalmente como a través de leyes especiales, muchos prefieren todavía ampararse en el recurso de habeas corpus, como ha sucedido por ejemplo en Chile.

Resulta en todo caso de gran interés remitirse a otros ordenamientos jurídicos, para de esta manera conocer cuales son las leyes que cada país dispone en caso de que se atente contra la vida íntima de los hombres, utilizando por ejemplo a Internet como medio para lograrlo.

---

[109] Citado por Oscar PUCCINELLI en El Habeas Data en Indoiberoamérica, pág. 351, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1999.

[110] Antonio PÉREZ LUÑO, Del "habeas corpus" al "habeas data", pág. 174, Editorial Aranzadi, Madrid, 1990-1991.

CAPÍTULO II: LA PROTECCIÓN DEL DERECHO A LA VIDA PRIVADA EN TRATADOS INTERNACIONALES Y EN EL DERECHO COMPARADO

A partir del término de la Segunda Guerra Mundial, muchos Estados optaron por caucionar internacionalmente los Derecho y Garantías inherentes al hombre, para con ello obtener su reconocimiento universal y por consiguiente alcanzar su debida protección. Dentro del ámbito de derechos reconocidos, el derecho a la protección de la vida privada comenzó a tomar forma, aun cuando en un principio su reconocimiento fuera poco profundo e incluso demasiado básico. Sin embargo, al pasar de los años, la Comunidad Internacional ha ido perfeccionando su alcance, y conforme la tecnología avanza, su ámbito de protección se ha ido ampliando de manera considerable.

En el caso del ordenamiento jurídico chileno, los Tratados Internacionales tienen rango constitucional [111], y muchos de los cuales describiremos a continuación tienen dentro de sus países miembros a Chile.

A continuación, una breve descripción de los Tratados creados por los principales organismos y comunidades internacionales, en cuanto protegen el derecho a la intimidad como derecho fundamental y el alcance que dicha protección ha tenido.

Tratados y Convenios Internacionales

Organización de las Naciones Unidas (ONU):

1.- Declaración Universal de Derechos Humanos:

La Declaración Universal de los Derechos Humanos de diciembre de 1948 establece en su artículo 12 que:

"Artículo 12.- Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques." [112] (subrayado es mío)

El citado artículo contiene una disposición sumamente amplia, que abre posibilidades de una interpretación extensiva. Tal característica es común a todas las normas contenidas en esta Declaración Universal de los

[111] El Artículo 5, inciso segundo de la Constitución Política de la República de Chile señala que: "El ejercicio de la soberanía reconoce como limitación el respeto a los derechos esenciales que emanan de la naturaleza humana. Es deber de los órganos del Estado respetar y promover tales derechos, garantizados por esta constitución y por los Tratados internacionales ratificados por Chile y que se encuentren vigentes".

[112] Organización de las Naciones Unidas. Declaración Universal de los Derechos Humanos. Nueva York. Diciembre de 1948.

Derechos Humanos, puesto que la intención del legislador internacional fue precisamente la de darle a este conjunto normativo la mayor amplitud interpretativa posible para que pudiera ser aceptado y aplicado por numerosos sistemas jurídicos internos. [113]

2.- Pacto Internacional de Derechos Civiles y Políticos:

En 1966, el derecho a la vida privada fue incluido en el Pacto Internacional sobre Derecho Civiles y Políticos, cuyo artículo 17 reza:

"Artículo 17.- 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".[114]

El precitado artículo conserva, como vemos, el espíritu de la Declaración Universal de los Derechos Humanos, y añade un elemento a la protección de la intimidad, estableciendo que no sólo deben proscribirse las "injerencias arbitrarias", sino también las "ilegales", lo cual implica al Poder Político en la preservación de la privacidad de los individuos.

3.- Convención Sobre los Derechos del Niño:

Esta Convención, partiendo de la base de los principios de libertad, justicia y de paz proclamados en la Carta de las Naciones Unidas, dispone que:

"Artículo 16.- Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y a su reputación.
El niño tiene derecho a la protección de la ley contra estas injerencias o ataques".[115]

Se trata de una Convención sumamente importante en cuanto a que se consagra por primera vez el derecho a la vida privada de los niños, contra injerencias arbitrarias o ilegales. De ello se desprenderán una serie de normas internas para garantizar este derecho en los diferentes países miembros.

4.- Directrices para la regulación de ficheros automáticos de Datos Personales:

---

[113]Ver a este respecto la obra de Alexander ROSEMBERG HOLCBLAT y Moriah SÁNCHEZ SANZ, El derecho a la privacidad en Internet, pág. 20, de texto publicado en http://vlex.com/redi/No. 37 - Agosto del 2001/5, visitada en diciembre del año 2001.

[114]Organización de las Naciones Unidas. Pacto Internacional sobre Derechos Civiles y Políticos. 1966.

[115] Asamblea General de la Organización de las Naciones Unidas, Convención Sobre los Derechos del Niño, celebrada con fecha 29 de enero de 1991.

La Subcomisión para la Prevención de la Discriminación y para la Protección de las Minorías elaboró ciertas directrices sobre ficheros de datos personales, en cuanto éstos tuvieren un tratamiento informatizado. Tales directrices fueron aprobadas mediante resolución de la Asamblea General de la ONU, el 29 de enero de 1991, y que tomaron como modelo las de la Organización para la Cooperación y Desarrollo Económico (OCDE) , a la cual nos referiremos más adelante.

Estas Directrices dejan las modalidades de aplicación de los reglamentos relativos a los ficheros llevados en forma computarizada a la iniciativa de cada Estado. Sin embargo, se establecieron una serie de principios que deberán respetarse por parte de cada legislación y que tendrán relación básicamente con: la licitud y lealtad de las informaciones relativas a las personas; su exactitud; su finalidad; no discriminación; seguridad; control y sanciones para quienes violen estos principios, posibilidades de acceso de las personas interesadas, entre otros ámbitos.

Dentro del conjunto de cláusulas que conforman esta normativa, es prudente nombrar la *Cláusula Humanitaria* porque justamente reconfirma la intención del legislador de proteger prioritariamente los derechos fundamentales de las personas.

"Cláusula humanitaria: debería preverse de manera específica una excepción a estos principios cuando el fichero tenga por finalidad proteger los derechos humanos y las libertades fundamentales de la persona de que se trate, o prestar asistencia humanitaria.

La legislación nacional debería contener una excepción análoga para las organizaciones internacionales gubernamentales en cuyo convenio sobre la sede no se hubiera excluido la aplicación de la legislación nacional, así como para las organizaciones internacionales no gubernamentales a las que sea aplicable dicha legislación".[116]

La importancia de esta cláusula recae básicamente en el hecho de que, a través de una visión futurista, se pretende desde ya amparar tanto en las legislaciones internas y externas de cada país el tráfico de ficheros de información con contenidos de relevancia constitucional. A través de la implementación de este tipo de principios, se incentivó a distintas legislaciones para dictar nuevas normativas destinadas a proteger especialmente derechos humanos como el derecho a la protección de la vida privada, y libertades fundamentales como la libertad de la autodeterminación informativa.

Organización de Estados Americanos (OEA).

1.- Declaración Americana de los Derechos y Deberes del Hombre:

[116]Asamblea General de la Organización de las Naciones Unidas, Directrices para la regulación de ficheros automáticos de Datos Personales, celebrada con fecha 29 de enero de 1991.

La Declaración Americana de los Derechos y Deberes del Hombre, primera declaración redactada en el siglo pasado en materia de Derechos Humanos señala que:

"Artículo 5.- Toda persona tiene derecho a la protección de la Ley contra ataques abusivos a su honra, a su reputación y a su vida privada y familiar. (...)

Artículo 10.- Toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia."[117]

Dentro de la doctrina hay quienes consideran que la interpretación de este artículo debe ser bastante amplia, postura interesante si se considera *exclusivamente* la protección de la correspondencia dentro del ámbito que conforma la vida privada de las personas. Es así que se ha señalado que: "El artículo 10 *supra* representa lo que podría llamarse el "standard" de la norma protectora del derecho a la privacidad de la correspondencia."[118]

2.- Convención Americana de Derechos Humanos:

A esta convención se la conoce también con el nombre de "Pacto de San José de Costa Rica", y en su artículo 11 declara que:

"Artículo 11.- PROTECCION DE LA HONRA Y DE LA DIGNIDAD

1.- Toda persona tiene derecho al respecto 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."[119]

Es notorio el hecho de que la regulación del derecho a la privacidad en esta Convención de 1969 toma su idea directamente del Pacto Internacional sobre Derechos Civiles y Políticos, pues es una copia casi fiel de su texto.

---

[117]Organización de Estados Americanos, IX Conferencia Internacional Americana, Declaración Americana de los Derechos y Deberes del Hombre, Bogotá, Mayo de 1948.

[118] Alexander ROSEMBERG HOLCBLAT y Moriah SÁNCHEZ SANZ, El derecho a la privacidad en Internet, pág. 20, de texto publicado en http://vlex.com/redi/No._37_-_Agosto_del_2001/5, visitada en diciembre del año 2001.

[119]Organización de Estados Americanos, Convención Americana de Derecho Humanos o Pacto de San José, Costa Rica. 22 de noviembre de 1969.

Organización para la Cooperación y Desarrollo Económico (OCDE):

Directrices para la Protección de la Privacidad y el Flujo Internacional de Datos Personales:

La OCDE es una organización internacional intergubernamental que reúne a los países más industrializados de economía de mercado, cuyas raíces se remontan a 1948, a través de la Organización para la Cooperación Económica Europea, encargada de administrar el Plan Marshall para la reconstrucción europea. El objetivo que persigue es estimular y desarrollar la economía y el comercio internacional; por ende, los estudios realizados en su seno tienen como fin último la identificación y análisis de las consecuencias que los nuevos desarrollos tecnológicos tienen en la economía y en el comercio mundial.

En 1978, se formó un Grupo de Expertos que elaboró un conjunto de Directrices, referentes a la intimidad personal y a las transmisiones internacionales de datos, que fueron adoptadas por el Consejo de Ministros de la OCDE, en forma de recomendación a los Estados miembros, el 23 de septiembre de 1980.

Su contenido es muy similar al del Convenio del Consejo de Europa sobre protección de datos, el cual será tratado más adelante. Ello ha contribuido a consagrar, en el ámbito internacional, cuatro normas jurídicas o principios básicos que deberán ser respetados en las transmisiones de datos, dentro de las fronteras de los Estados, o entre éstos. En relación a las transmisiones internacionales de datos, estas Directrices recomiendan a los siguientes principios:

"a) los Estados deben tener en cuenta las implicaciones del procesamiento interno y reexportación de datos personales a otros Estados (parágrafo 15). El énfasis de esta cláusula pone de relie ve la necesidad de un respeto mutuo entre los Estados en el área de la protección de datos personales y la vida privada. Ello implica que la normativa nacional sobre transferencias internacio nales de datos no debe estar destinada a eludir o violar las regulaciones de otros Estados en materia de protección de datos personales y vida privada;

b) cada Estado debe tomar las medidas razonables y apropiadas para que las transmisiones internacionales sean ininterrumpidas y seguras, incluso cuando se realizan a través del territorio de un Estado miembro (esta cláusula no es más que la extensión del principio básico de seguridad a la transmisión internacional de datos);

c) los Estados deben evitar, en general, restringir las transferencias internacionales de datos personales, excepto cuando: 1) los Estados receptores "no observen" el contenido de las Directrices; 2) cuando la reexportación de datos personales eluda las disposiciones internas del Estado transmisor; ó 3) cuando ciertas categorías de datos personales -e.g. datos sensibles- reciban una protección especial en la legislación interna y tal protección no sea equivalente en otros Estados;

d) los Estados deben evitar adoptar disposiciones normativas, políticas y prácticas legales cuando: 1) la única finalidad sea proteger la intimidad y las libertades individuales, si para ello se obstaculiza la transmisión internacional de datos; 2) el contenido de las disposiciones exceda de la normativa ya existente

sobre el tema. Con esta cláusula, las Directrices intentan buscar un equilibrio entre la protección de la intimidad y la libre circulación internacional de información."[120]

En 1985, la OCDE adoptó una declaración sobre las transferencias internacionales de datos no personales y posteriormente creó una comisión sobre informatización automatizada y privacidad para estudiar una posible revisión de las Directrices de 1980.[121]

Consejo de Europa.

1.- Convención Europea de Derechos Humanos:

Esta convención, que a nivel europeo marcó la pauta de importantes futuras convenciones, se celebró con fecha 3 de septiembre de 1953, y en su artículo 8 dispone que:

"Artículo 8: 8.1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia;

8.2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto y en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".[122]

Este artículo, en su primer punto, tiene una redacción bastante parecida en relación a lo que se proclama en las Declaraciones de la OEA y de la ONU. Esta similitud responde a una ola de reconocimiento de derechos humanos. Es curioso que, a pesar de su amplio alcance, no pasarán sino poco más de tres décadas para que el Consejo de Europa se viera obligado a crear una norma que se adapte a las nuevas necesidades de protección del derecho a la vida privada, a través del Convenio 108, el cual será explicado a continuación.

2.- Convención 108 sobre la protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal:

Este Convenio es el producto de todo un proceso que culminó el 15 de noviembre de 1985 y que se remonta al año 1968, fecha en que la Asamblea Parlamentaria del Consejo de Europa emitió una llamada al Consejo de Ministros para que éste examinara si las legislaciones internas de los Estados miembros protegían

[120] Organización para la Cooperación y Desarrollo Económico, Directrices para la Protección de la Privacidad y el Flujo Internacional de Datos Personales, 23 de septiembre de 1983.
[121] Para más información, remitirse a la obra de Mercedes URIOSTE, Protección de Datos Personales, de Revista de la Secretaría de Derecho Comparado de la Corte Suprema de la Nación Argentina, pág.5,de texto publicado en http://comunidad.derecho.org/redi/Habeas6.zip, visitado en enero de 2002. Este texto será citado frecuentemente porque es una fuente muy completa de información.
[122] Consejo de Europa, Convención Europea de Derechos Humanos, 3 de septiembre de 1953.

adecuadamente el derecho de los individuos al respeto de la vida privada, dado el creciente desarrollo de las tecnologías informáticas.[123]

El resultado de este estudio demostró que las legislaciones nacionales no estaban plenamente adaptadas a los cambios introducidos por las nuevas tecnologías de la información, por lo que se constituyó un Comité Intergubernamental de expertos encargados de elaborar las medidas apropiadas a nivel regional europeo. De este Comité emanaron las pautas que en 1973 y 1974 inspiraron la aprobación, por parte del Consejo de Ministros, de dos resoluciones sobre la protección de la vida privada de los individuos con respecto a los bancos electrónicos en el sector privado (Res. 73/22) y público (Res. 74/29). Estas resoluciones tienen importancia histórica, ya que son los primeros textos supranacionales donde se recogen "pautas de conducta" para los Estados sobre la protección de datos.

Para 1976, el Comité de Ministros adoptó una resolución con el objeto de constituir un Comité de Expertos de protección de datos, el cual se encargaría de perfeccionar el alcance del artículo 8 de la Convención Europea de Derechos Humanos, con el fin de ampliar su aplicación no solo a los Estados miembros. Su propósito principal sería garantizar a las personas naturales, independientemente de su nacionalidad o residencia, el respeto a sus derechos fundamentales y en particular, la protección del derecho a la vida privada frente al desafío que se planteaba con la automatización de datos de carácter personal.[124] A grandes líneas, lo que se logró a través de esta normativa fue establecer una reglamentación en cuanto al tratamiento, seguridad y transmisión de datos de carácter personal, novedoso para la época, y que serviría de base para futuras reglamentaciones.

3.- Directiva 95/46 sobre la protección de los individuos en relación al procesamiento de datos personales y sobre libre circulación de esos datos.

Esta Directiva se llevó a cabo el 24 de octubre de 1995. Con la llegada de la llamada "sociedad informática", el tratamiento de datos de carácter personal requeriría de una reglamentación clara frente a un mercado interno y externo libre de fronteras. A través de esta Directiva, se buscó modificar las legislaciones internas de cada país, con el fin de que el derecho a la intimidad fuera equivalente dentro de toda la Comunidad. Es así que se llevó a cabo el desarrollo internacional más importante en la materia. En tal sentido, a modo de resumen se puede señalar que tal Directiva:

a) establece los principios para la protección de la privacidad a nivel europeo que deben ser incorporados a la legislación de todos los Estados miembros. Por lo tanto, representa el más modemo

[123] Recomendación 509, celebrada en la 3° parte de la XIX cesión, 1968. Ver también a este respecto la obra de Eduardo NOVOA MONREAL, Derecho a la vida privada y Libertad de Información, Siglo XXI Editores SA de CV, México D.F., cuarta edición, 1989, pág. 37.

[124] Ver también a este respecto los comentarios sobre este convenio de Mercedes URIOSTE en Protección de Datos Personales, de Revista de la Secretaría de Derecho Comparado de la Corte Suprema de la Nación Argentina, pág.6,de texto publicado en http://comunidad.derecho.org/redi/Habeas6.zip , visitado en enero del 2002.

consenso internacional sobre el contenido deseable del derecho a la protección de datos y constituye un modelo valioso para otros países y,

b) prohíbe la transferencia de datos personales desde la Comunidad a cualquier Estado no miembro que no tenga leyes de protección de datos "adecuadas"[125], lo cual impone un grado de presión internacional para que aumente el nivel de protección en los demás países, particularmente en el sector privado.

El análisis de esta Directiva merece especial detenimiento, pues de ella derivarán las directrices de lo que serán las posteriores dos Directivas en cuanto a las normas de procedimiento se refieren. Según esta reglamentación, está prohibido el procesamiento de datos que "revelen el origen étnico o racial, las opiniones políticas, las convicciones filosóficas o religiosas, las pertenencias a sindicatos, la salud, o la vida sexual" (art. 8). Hago mención de este punto, porque para esta normativa, los llamados *datos sensibles* se vuelven, a través de su específico nombramiento, más amplios que los que muchas legislaciones consideran como tales.

Dentro de este ámbito, la búsqueda de una aproximación legislativa entre los países miembros se ha vuelto una tarea ardua y vital. Por ello, otra de las grandes novedades que aportó esta Directiva fue la de proponer a sus miembros la creación de una o más autoridades públicas que se encarguen de velar por la debida aplicación de las normas propuestas, con el objeto de que actúen con "completa independencia", con "poderes efectivos de investigación" en el procesamiento (art. 28).

Así mismo, los Estados miembros deben alentar a la elaboración de *códigos de conducta*, de acuerdo a las particularidades de cada sector. Estos códigos están destinados a contribuir a la correcta aplicación de las disposiciones nacionales adoptadas por aquellos Estados en aplicación de esta Directiva. Además les corresponde establecer que las asociaciones profesionales y las demás organizaciones representantes de otras categorías de responsables de tratamientos que hayan elaborado proyectos de códigos nacionales, o que tengan la intención de modificar o prorrogar códigos nacionales existentes, puedan someterlos al dictamen de las autoridades nacionales para ver si cumplen con las leyes nacionales, según lo establece su artículo 27. El plazo establecido para que los Estados miembros adecuen sus leyes según las exigencias de esta Directiva es de tres años, a partir de su adopción, de acuerdo al artículo 32 de dicho cuerpo legal.

Se crearía un ente fiscalizador a nivel supranacional, dividido en tres organismo: la Comisión de la Comunidad, un Comité de Representantes de los Estados miembros de la Unión (y en algunas circunstancias

[125] Según el art. 25.2, "el carácter adecuado del nivel de protección que ofrece un tercer país se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países". El art. 26.6 declara que la Comisión puede decidir que un tercer país "asegura un nivel adecuado de protección... a la vista de su legislación o de los compromisos internacionales que ha asumido especialmente al término de las negociaciones [que ha mantenido con la Comisión]".

el propio Consejo de la Comunidad) y un *Working Party*[126] que tiene por objeto la protección de las personas respecto al Procesamiento de Datos Personales.

La directiva 96/9 de la Comunidad Europea no sería sino un perfeccionamiento de la Directiva anterior en cuanto a protección de las Bases de Datos, por lo cual merece mayor atención la Directiva 97/66/CE, ya que trata puntos más acordes con esta tesis.

4.- Directiva 97/66/CE del Parlamento Europeo y del Consejo sobre procesamiento de datos en el sector de las telecomunicaciones dentro de la Comunidad.

Esta Directiva se celebró con fecha 15 de diciembre de 1997, en la cual temas como la regulación del correo electrónicos y normas para las nuevas tecnologías serían analizados. Es así que el artículo primero de esta Directiva proclama que el objetivo principal será: "Armonizar las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de los derechos y libertades fundamentales, y en particular del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las telecomunicaciones, así como a la libre circulación de tales datos y de los equipos y servicios de telecomunicaciones en la Comunidad."[127]

Se desprende claramente que existe una necesidad de proteger el derecho a la vida privada frente a la amenaza que representan los nuevos medios de comunicación. Es un avance notable en el sentido de que se comienza a enfocar el problema desde el punto de vista de las *telecomunicaciones*[128], pues el ámbito de protección claramente busca sobrepasar lo que hasta entonces comprendían los simples medios de comunicación.

El artículo quinto reconoce por su parte, el poderío que estos medios de telecomunicación representan en cuanto a la invasión de la intimidad de las personas, por lo cual dispone que:

"Artículo 5.- Los Estados miembros garantizarán, por medio de normas nacionales, la confidencialidad de las comunicaciones efectuadas a través de las redes públicas de telecomunicación y de los servicios de telecomunicación accesibles al público". [129]

---

[126] El *Working Party* está integrado por un representante de la autoridad de protección de datos de cada Estado parte, un representante de las instituciones de la Comunidad, y un representante de la Comisión (art. 29). Toma sus decisiones por mayoría simple. Del mismo modo, examina la uniformidad de las leyes nacionales dentro de la Comunidad, da su opinión sobre el nivel de protección que existe en la Comunidad y en terceros países y sobre los códigos de conducta elaborados a nivel comunitario, y asesora a la Comisión sobre las medidas adicionales propuestas. También puede hacer recomendaciones de oficio sobre todas las cuestiones relativas al procesamiento de datos personales dentro de la Comunidad. El *Working Party* tiene que publicar un informe anual sobre el procesamiento de datos personales en Europa y en los terceros países (art. 30).

[127] Artículo primero del Consejo de Europa, Directiva 97/66/CE del Parlamento Europeo y del Consejo, 15 de diciembre de 1997.

[128] El Diccionario de la Lengua Española define a Telecomunicación como el "Sistema de comunicación telegráfica o radio telegráfica, y demás análogos". Real Academia Española, Vigésima Primera Edición, Madrid, 1992,pág. 1384.

[129] Ibídem, artículo quinto.

Obviamente que dentro de los "servicios de telecomunicación accesibles al público" están las comunicaciones a través de Internet y de la telefonía celular. Es también una puerta abierta frente a posibles nuevas tecnologías electrónicas entre las personas. Este artículo confirma así mismo la intención de la Directiva de buscar una protección de la intimidad a nivel comunitario.

En cuanto a la protección de Datos Personales, se dispone que:

"Artículo 11.- Los datos personales que figuren en las guías de los abonados, impresas o electrónicas, a disposición del público o que se puedan obtener a través de servicios de información que refieran a la guía, deberán limitarse a lo estrictamente necesario para identificar a un abonado particular, a menos que el abonado haya dado su consentimiento inequívoco para que se publiquen otros datos personales". [130]

Se vuelve interesante el hecho de que esta Directiva, conciente del valor que han adquirido el almacenamiento y comercialización de las bases de datos de las personas, pretenda proteger el malogrado uso que ellas puedan tener. Un ejemplo de ello es la indiscriminada transmisión de información con fines de *marketing*, al volverse definitivamente una serie de informaciones sin trascendencia bien organizadas en un cotizado bien dentro de las empresas a nivel mundial.

Otros Tratados Internacionales:

1.- Conferencia de Países Nórdicos (conocida también como Conferencia de Juristas Nórdicos):

Se llevó a cabo los días 22 y 23 de mayo de 1967 en la ciudad de Estocolmo. Se celebró como iniciativa de la sección sueca de la Comisión Internacional de Juristas, y de la cual participaron juristas de todas partes del planeta. Tuvo dentro de sus principales objetivo el delimitar con la mayor precisión posible, a través de una cuantiosa lista las formas, los medios y los procedimientos que representen una amenaza al derecho a la protección de la vida privada de las personas. Dicha enumeración ha sido calificada por muchos estudiosos del tema como "exitosa" para la época[131].

---

[130] Ibídem, artículo undécimo.

[131] Se consideraría en esta Conferencia que "el derecho a la vida privada de un individuo significa estar protegido de: a) injerencias en su vida privada, familiar, y de hogar; b) injerencias en su integridad mental o física o su libertad moral o intelectual; c) ataques a su honra o a su reputación; d) verse colocado en situaciones equívocas; e) la revelación, fuera de propósito, de hechos penosos de la vida privada, f) el uso del nombre, identidad o semejanza; g) ser copiado, atisbado, observado y acosado; h) violaciones a su correspondencia; i) abuso de medios de comunicación, escritos u orales; j) revelación de información dada o recibida en virtud del secreto profesional.

En este documento internacional, el alcance que se da a este derecho se resume en que "en la sociedad moderna, el respeto a la vida privada, como cualquier otro derecho del hombre, no puede ser ilimitado, salvo en el sentido de que nada puede justificar medidas incompatibles con la dignidad física, mental, intelectual o moral de la persona humana. Los límites que son necesarios para asegurar el equilibrio entre los intereses del individuo con los de otros individuos, grupos y el Estado, variarán según la situación en la que se busque dar efecto al derecho a la intimidad". [132]

Sin embargo, en la actualidad hay quienes creen, como Novoa Monreal, que debe verse como una postura doctrinaria obsoleta en el sentido de que se "incurre en el uso de expresiones de índole general, que no indican ningún contenido concreto", así como también por el hecho de "incluir aspectos que corresponden a otros derechos humanos, que en su oportunidad se diferirán del derecho a la vida privada".[133]

2.- Proclamación de Teherán de Derechos Humanos de 1968.

Se trata de una Proclamación que tuvo dentro de sus objetivos principales el que los Estados miembros de la Organización de las Naciones Unidas fomenten y estimulen el reconocimiento de los derechos fundamentales. En esta reunión, fueron analizados muchos trabajos tendientes a proteger a la vida privada, sobre todo con el objetivo de ampararla frente a las nuevas tecnologías y al avance de la civilización. Era la primera vez que se consideraba de una manera tan concreta las potenciales amenazas de la nueva era frente a los derechos fundamentales.

Dentro de las conclusiones notables que se manifestaron es la que señala que "el derecho a la vida privada en tanto que derecho al respeto de la intimidad representa una realidad superada, porque las necesidades de las personas se orientan a la defensa del ejercicio de determinadas libertades individuales o colectivas de carácter económico, social, cultural o político".[134] Según Puccinelli, uno de los principales aportes de esta Proclamación es que sería la primera vez que se pretendería proteger los datos personales de las personas.[135]

De esta iniciativa se darían pie a una serie de proyectos, cuyos esfuerzos se verían reflejados en la Asamblea General de la ONU, celebrada en 1990, que estableció una serie de principios rectores para la reglamentación de ficheros computarizados de datos personales.

---

[132] Citado por Ana Isabel HERRÁN ORTIZ, La violación de la intimidad en la protección de datos personales, pág. 55, Editorial Dykinson, Madrid, 1998.

[133] Eduardo NOVOA MONREAL, Derecho a la vida privada y Libertad de Información, Siglo XXI Editores SA de CV, México D.F., cuarta edición, 1989, pág. 30.

[134] Citado por Ana Isabel HERRÁN ORTIZ, La violación de la intimidad en la protección de datos personales, pág. 56, Editorial Dykinson, Madrid, 1998.

[135] Ver a este respecto la obra de Oscar PUCCINELLI, El Habeas Data en Indoiberoamérica, pág. 139, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1999

Derecho Comparado

En diversos países del mundo, la protección del derecho a la vida privada se ha visto consagrada no solo a través de Tratados Internacionales, sino que a través de las propias Cartas Fundamentales y leyes o decretos internos. Tal protección ha sido muy variada en relación a cada país, marcando tendencias bastantes distintivas entre estados europeos y americanos.

Sin embargo, dentro de este conjunto de normas, la protección del derecho a la intimidad frente a la llegada de las nuevas tecnologías, más precisamente Internet, parece no haber sido suficiente. Es por ello que, después de la ola legislativa que se produjo en el mundo por consagrar el derecho de *Habeas Data*, en la actualidad son varios los proyectos de ley que pretenden regular precisamente una normativa destinada a proteger el derecho de los hombres por conservar su vida privada alejada de la invasión de las nuevas tecnologías y medios de telecomunicación.

Pretendiendo seguir este patrón, a continuación haré un muy breve análisis de las normas existentes en diversos países del mundo, buscando de esta manera estudiar los reconocimientos constitucionales, nombrar las principales características que se consagran con el recurso de Habeas Data y los proyectos de ley existentes en algunos países del planeta, por sobre todo, en lo referente a la protección del derecho a la intimidad frente al desafío que presentan los nuevos medios de comunicación electrónicos.

Europa

1.- Italia

Normas Constitucionales:

La Constitución de la República italiana fue aprobada por la Asamblea Constituyente el 22 de diciembre de 1947, y entró en vigor el 1 de enero de 1948. En sus artículos 13, 14 y 15 desarrolla lo que es el derecho a la libertad personal y a la intimidad.

"Artículo 13º. La libertad personal es inviolable. No se permite forma alguna de detención, de inspección o de registro personal, ni cualquiera otra restricción de la libertad personal, sino por resolución motivada de la autoridad judicial y solamente en los casos y en las formas previstos por la ley.
En casos excepcionales de necesidad y urgencia, indicados taxativamente por la ley, las autoridades de la seguridad pública podrán adoptar medidas provisionales que deben ser comunicadas dentro de cuarenta y ocho horas a la autoridad judicial y, si ésta no las convalida en las sucesivas cuarenta y ocho horas, se entenderán revocadas y quedarán privadas de todo efecto.

Está castigada toda violencia física o moral sobre las personas sometidas a restricciones de libertad. La ley establecerá los límites máximos de la detención preventiva.

Artículo 14º. El domicilio es inviolable. No pueden realizarse inspecciones, registros o secuestros a no ser en los casos y en las formas establecidos por la ley según las garantías establecidas para la tutela de la libertad personal.

Las verificaciones y las inspecciones por motivos de sanidad y de incolumidad públicas o para fines económicos y fiscales se regularán por leyes especiales.

Artículo 15º. La libertad y el secreto de la correspondencia o de toda otra forma de comunicación son inviolables.

Su limitación solamente puede tener lugar por resolución motivada de la autoridad judicial con las garantías establecidas por la ley."[136] (subrayado es mío).

Aunque la Constitución italiana no contiene normas específicas sobre la protección del derecho a la intimidad, sí crea una base jurídica en la que, al protegerse el derecho a la libertad personal, a la inviolabilidad del hogar y a la inviolabilidad de la correspondencia, puede deducirse que, por analogía, se protege constitucionalmente la intimidad de las personas. Este aparente vació se verá llenado con las distintas leyes internas, en especial las normas sobre protección de datos recientemente creadas.

Normas internas:

La ley más importante es la N° 675 del 31 de diciembre de 1996 en italiano *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali,* la cual tiene por objeto adecuar la legislación italiana a la Directiva 95/46/EC. También contiene las disposiciones necesarias para implementar el Convenio 108 del Consejo de Europa que -ratificado en marzo de 1997- entró en vigencia en Italia el 1 de julio de ese mismo año. Por otra parte, en la misma fecha y a través de la ley 676, el Parlamento autorizó al gobierno a dictar normas reglamentarias para modificar y complementar la mencionada ley 675.

Una de las mayores novedades que presenta esta ley es la creación de dos figuras especiales: el *Controlador de los* Datos y *el Procesador de los Datos.*

Según el artículo 1.2, en su literal d, "El Controlador es la persona natural o jurídica, autoridad, organismo o ente público, asociación u organización, que determina los objetivos y forma del procesamiento de los datos personales, incluso las medidas de seguridad", mientras que "El Procesador es la persona natural

[136]Artículos 13, 14 y 15 de la Constitución de la república Italiana, cuya información se obtuvo en Constituciones del Mundo. http://www.cepc.es, visitada en marzo del 2002.

o jurídica, autoridad, organismo o ente público, asociación u organización, que procesa los datos personales en nombre del Controlador (art. 1.2.e)."[137]

En cuanto al objeto de esta ley, está destinada a asegurar que los procesamientos de datos personales respeten los derechos y libertades fundamentales y la dignidad de las personas naturales, particularmente su derecho a la intimidad e identidad personal, y también los derechos de las personas jurídicas y de cualquier otro organismo o asociación (art. 1.1), siendo a este respecto, por ende, más amplia que la Directiva y el Convenio mencionados. Esto representa una importante novedad en el sentido de que se considera a la *identidad personal* como un medio digno de protegerse para garantizar adecuadamente el resguardo y el desarrollo de la intimidad de las personas. Además, protege la vida privada de las *personas jurídicas*.

Otra de las importantes novedades de esta ley es que se aplica a los procesamientos de datos -por medios electrónicos o no (art. 5.1)- que se realizan en territorio italiano, con indiferencia de quién los realice (art. 2.1), incluso cuando los datos se encuentran en el extranjero, en cuyo caso siempre se aplican las normas que regulan la transmisión de datos al exterior (art. 6). Efectivamente, el legislador está conciente del peligro que representan tanto Internet como otros medios electrónicos, y el hecho de que se los haya considerado específicamente es ya un primer paso.

La transferencia de datos al exterior está consagrada en el artículo 28 de la citada ley, el cual señala que:

"Artículo 28: 1)La transmisión aun transitoria de datos sometidos a procesamiento al extranjero, cualquiera sea su forma o instrumentación, debe notificarse previamente a la Autoridad cuando el país de destino no es miembro de la Comunidad Europea, o la transferencia incluye datos sensibles o los mencionados en el art. 686 del Código de Procedimientos Penal. (...)

3) Está prohibida la transmisión cuando las leyes y regulaciones del país de destino no garantizan a los interesados un adecuado nivel de protección o, al menos, la misma protección que la presente ley en el supuesto en que la transmisión incluya datos sensibles o los mencionados en el art. 686 del Código de Procedimientos Penal."[138]

Junto con el Controlador y el Procesador de datos, existe también la *Autoridad de Contralor para la Protección de las Personas Naturales y de otros Sujetos en relación al Procesamiento de Datos Personales* (Autoridad), que cumple sus funciones con completa independencia de criterio y apreciación . Se trata de un cuerpo colegiado de 4 miembros, elegidos en partes iguales por cada una de las Cámaras del Congreso, que escoge a uno de ellos como Presidente. El voto de este último define en caso de paridad. Los integrantes de la Autoridad deben mostrar independencia y ser expertos de reconocida trayectoria en las disciplinas del

[137] Artículo 1.2 de la Ley 675 *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali* de la República de Italia.

[138] Artículo 28 de la Ley 675 *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali* de la República de Italia.

derecho o tecnología informática. Duran 4 años en sus funciones, y son reelegibles sólo una vez. Además, su dedicación es exclusiva.[139]

Aparte de la Ley 675, existen los decretos 123 y 255, del 9 de mayo y 28 de julio de 1997 respectivamente, que complementan esta ley en relación a la información y a las notificaciones simplificadas.

Entre los instrumentos legislativos que gobiernan cuestiones anexas a las antes mencionadas, vale señalar la Convención Europea de Europol -que da a la Autoridad la responsabilidad sobre los datos personales que constan en archivos nacionales-, y la ley que instituye la *Autorita per le garanzie nelle Comunicazioni*, relativa a la coordinación de las actividades de las autoridades de contralor y a la posibilidad que tiene el Consejo de Usuarios Nacionales de someter sus opiniones y sugerencias a la Autoridad.

Con el objeto de complementar la Ley 675, llamada también *Ley Madre* respecto de la protección de datos de carácter personal, en julio de 1999 entró en vigencia en Italia el Decreto Presidencial Nº 318 o decreto 318/99. Dicho Decreto fue dictado en cumplimiento del mandato de la Sección 15, parágrafo 2do, de la Ley de Protección de Datos italiana de 1996 y entró en vigencia en marzo de 2000. El objeto del Decreto 318/99 es regular una lista de requerimientos mínimos que deben ser observados al procesar datos personales. Estos requerimientos son, además, asegurados por las normas contenidas en la ley que exige su creación, es decir, la Ley 675.

En cuanto a la implementación de la Directiva de Protección de Datos de la Unión Europea en Italia (Directiva 97/66/EC), el gobierno italiano la hizo parte de su Derecho Interno mediante el Decreto Legislativo 171/98. Dicha Ley tiene por objeto regular la protección de los datos en el sector de las telecomunicaciones, y debe ser interpretada y aplicada en concordancia con la Ley 675 de 1996. Por lo tanto, las disposiciones generales de la Ley 675 consagran la obligación de informar a los sujetos de los datos sobre el procesamiento de los mismos; obtener su consentimiento cuando sea necesario; y adoptar todas las medidas de protección necesarias para evitar el acceso no autorizado a los datos personales; siguiendo todo ello en vigencia con la entrada en vigor de esta nueva Ley 171/98.

La intervención de teléfonos está regulada en los códigos Penal (arts. 614 a 623) y de Procedimientos Penal (arts. 266 a 271), que requieren orden judicial, la cual, en la mayor parte de los casos, puede tener una vigencia de 15 días.

Existe además una innovación en el Código Penal italiano, donde a través del Acta N°305/93, que modificó el artículo 616 de ese cuerpo legal, se ha pretendido dar protección a las comunicaciones por correo electrónico y demás alternativas telecomunicacionales, adelanto sin duda notable y moderno.[140]

---

[139] Ello se desprende del artículo 30 de la Ley 675 *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali* de la República de Italia.

Existen también leyes sectoriales relativas a supervisión en los lugares de trabajo (Ley N° 93, del 29 de marzo de 1983, *Legge quadro sul pubblico*), a información estadística, a archivos electrónicos y firmas digitales (Decreto Presidencial N° 513, del 10 de noviembre de 1997).

Sin duda alguna que la normativa italiana tendiente a proteger el derecho a la intimidad de las personas es una de las más avanzadas de Europa y del mundo, pues se ajusta plenamente a las exigencias internacionales, sobre todo a la de la Unión Europea. Además, dentro de sus leyes internas es ejemplar el reconocimiento que se hace frente a la amenaza que representa la tecnología, tanto para las personas naturales como jurídicas, lo cual también es novedoso y actual.

2.- Alemania

Normas Constitucionales:

La Carta Magna germana en su artículo décimo consagra el derecho al secreto de las comunicaciones. No es precisamente un reconocimiento al derecho a la intimidad, sino que la norma sólo abarca una parte de éste. Luego de la reunificación de las dos Alemanias, se revisó el texto de la Constitución y de hecho existió la intención de consagrar el derecho a la vida privada dentro de su normativa. Sin embargo, el proyecto no tuvo el apoyo suficiente de la entonces mayoría conservadora.

"Articulo 10.o. :1. Será inviolable el secreto de la correspondencia (Briefgeheimnis), así como el del correo y los telégrafos.

2. Solo en virtud de una ley podrán establecerse limitaciones a este derecho. Si la restricción obedece al propósito de proteger el orden básico liberal y democrático o la existencia o salvaguardia de la Federación o de un Estado regional, podrá la ley disponer que no se comunique la restricción al afectado y que el control sea asumido por órganos y auxiliares designados por la representación del pueblo, en vez de correr a cargo de la autoridad judicial." [141]

El primer punto de este artículo resulta interesante desde la perspectiva de que por analogía, se entiende que el correo electrónico se encuentra protegido por la Constitución, al protegerse el "secreto de la correspondencia".

---

[140] Información obtenida en el artículo "Privacy Laws & Business International Data Protection Roundup", de la revista la revista Privacy Laws&Bussines, International Newsletter, N° 60, de edición de enero del 2002, pág. 17.

[141] La traducción de este artículo en alemán es "Artikel 10 [Brief-, Post- und Fernmeldegeheimnis] (1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich. (2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt", de texto obtenido en http://www.estudionuner.com.ar/legislacion.htm, visitado en marzo de 2002.

Normas Internas:

La primera ley estadual fue la del Estado de Hessen del 7 de octubre de 1970 sobre Protección de Datos. Sin embargo, a nivel federal, se comenzó con la aprobación de la *Federal Data Protection Law* de 1977, luego sustituida por la *Federal Data Protection Act* de 1990.[142] Esta ley tiene por objeto el regular la recolección, procesamiento y uso de datos personales que hacen los entes públicos federales y estaduales (estos últimos en la medida en que no estén regulados por la legislación estadual y siempre que apliquen leyes federales). También se aplica al procesamiento o uso de datos personales que hacen los particulares en el curso normal de su gestión comercial o profesional (Secs. 1.1 y 1.2). Sin embargo, su aplicación es supletoria a la de otras normas que regulan la protección de los datos personales o su publicación, pero sus disposiciones prevalecen sobre las de la Ley de Procedimiento Administrativo en la medida en que se procesen datos para evaluar hechos (Sec. 1.5).

En el primer punto de la sección tercera de esta ley, el titular de la protección es "la persona física identificada o identificable". Uno de los puntos más notables dentro de esta normativa es el rol que juega el sujeto pasivo, vale decir el potencial afectado. Es así que la Sección cuarta establece que:

"Sección 4: El interesado debe saber, antes de prestar su consentimiento, el objeto del almacenamiento, los destinatarios de los datos, y si lo solicita, los efectos de no dar su autorización Dicho consentimiento debe ser escrito -a menos que por circunstancias especiales sea mejor prestarlo de otro modo- y estar claramente diferenciado cuando forme parte de otras declaraciones escritas".[143] (subrayado es mío).

Esto también es poco común en muchas legislaciones, ya que generalmente no se considera la opinión del afectado, la cual pasa a ser secundaria cuando existen intereses pecuniarios de por medio. Además, el hecho de exigirse el consentimiento -por regla general por escrito- del interesado es un excelente medio probatorio cuando se ha violado la vida privada de las personas sin su aceptación. Solo se permite el tratamiento de datos personales sin la venia del interesado en los casos previstos por la Ley. Esto se aplica tanto para los entes públicos como privados, así como para fines investigativos como de mercado o publicitarios. Esto se vuelve fundamental a la hora de buscar protección frente al indiscriminado uso de los bancos de datos a través de Internet por ejemplo, ya que en una inmensa mayoría de los casos, la recolección de datos concernientes a la vida privada de las personas ni siquiera contempla la posibilidad de notificárselo a los afectados.

En otro ámbito, la sección 18 de la Ley se ha preocupado de implementar la protección de datos en la Administración Pública Federal.

---

[142] El texto de esta norma se obtuvo de la obra de Mercedes URIOSTE en Protección de Datos Personales, de Revista de la Secretaría de Derecho Comparado de la Corte Suprema de la Nación Argentina, pág.6,de texto publicado en http://comunidad.derecho.org/redi/Habeas6.zip, visitado en enero del 2002.

[143] Sección 4 de la *Federal Data Protection Act* de la República de Alemania.

"Sección 18.- Las Supremas Autoridades Federales, el Presidente del Fondo Federal Especial Ferroviario, así como los organismos, establecimientos y fundaciones de derecho público que sólo están sujetos a la supervisión del Gobierno Federal o de una Suprema Autoridad Federal, tienen que asegurar la implementación de esta Ley y de las otras normas relativas a la protección de datos en sus respectivas áreas de actividad.

Lo mismo se aplica al directorio de las empresas establecidas por ley, en la medida en que tienen un derecho exclusivo en términos de la Ley de Administración Postal o de la Ley de Instalación de Telecomunicaciones.

Los organismos públicos deben llevar un registro de los sistemas de procesamiento de datos que usan, y dejar allí constancia escrita de la siguiente información: designación y tipo de archivos de datos; objeto; tipo de datos almacenados; interesados; tipos de datos que regularmente se transmiten y sus receptores; períodos estándares para la supresión de datos; grupos de personas que tienen derecho de acceso o las personas que tienen este derecho en forma exclusiva (...)". [144](subrayado es mío).

Esta norma se vuelve interesante en cuanto a las obligaciones que podrían recaer en los Proveedores de Servicios de Internet, más conocidos como ISP (cuyas siglas en inglés son Internet Service Porvider)[145]. Así mismo, si acaso los sistemas de procesamiento utilizados tienen relación con Internet, es más fácil controlar el uso que se le está dando esta poderosa herramienta de almacenamiento y comunicación de información.

Dentro de las obligaciones del Comisionado, se encuentra la de supervisar la protección de los datos personales sujetos a secreto profesional u oficial especial, especialmente el secreto impositivo, pero esta facultad no alcanza a los amparados por el secreto de la correspondencia y de las telecomunicaciones, a los datos médicos, a los incluidos en registros personales, y a los asuntos no administrativos de los tribunales federales (Sec. 24.2 y 24.3).

Conjuntamente con el Comisionado está la *Autoridad de Contralor* (Autoridad), la cual supervisa en un caso determinado la observancia de esta ley y de las otras relativas a la protección de datos, cuando tiene suficientes indicaciones de que han sido violadas y, particularmente, cuando el interesado presenta prueba en este sentido(Sec. 38.1).

Los entes sujetos a su contralor, deben brindarle toda la asistencia necesaria para el cumplimiento de sus funciones. A fin de garantizar la protección prevista en esta ley, la Autoridad puede exigir la adopción de las medidas que considere oportunas. Al referirse al manejo de información personal, casi todas las leyes alemanes remiten a la ley de protección de datos aplicable o contienen secciones especiales para este área.

---

[144] Sección 18 de la *Federal Data Protection Act* de la República de Alemania.

[145] Debe entenderse por PSI a los Proveedores de Servicios de Internet, cuyas siglas en inglés son ISP a toda "Organización, habitualmente con ánimo de lucro, que además de dar acceso a Internet a personas fpisicas y/o jurídicas, les ofrece una serie de servicios (por ejemplo, hospedaje de páginas web, consultoría de diseño e implementación de de webs e intranets, etc,). Definición obtenida de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

Muy recientemente se han aprobado varias normas relativas a la privacidad de las comunicaciones, como la *Telecommunications Carriers Data Protection Ordinance (TDSV)*, que entró en vigencia el 18 de diciembre del 2000 y cuyo aporte se ha visto reflejado en la regulación de las relaciones entre proveedores de servicios y particulares. También está la *Information and Communication Services (Multimedia) Act* de 1997 protege la información usada en redes informáticas y establece las exigencias jurídicas que deben cumplir las firmas hechas en forma digital.

Con fecha 29 de enero del 2002 se promulgó en Alemania la *Interception of Telecommunicatios ordinance (Telekommunikations-Überwachungsverordung- TKÜV)*, que dentro de sus particularidades obliga a compañías privadas a equipar y mantener equipos comunicacionales que puedan ser interceptados por autoridades del gobierno. Entre sus adelantos está un significante desarrollo en cuanto al establecimiento de un código que permita identificar las comunicaciones que se llevan a cabo a través de este medio. Sin embargo, esta nueva ley tiene también varios detractores.[146]

Es necesario mencionar que Alemania aún no ha aprobado una nueva ley de protección de datos que se conforme a la Directiva 95/46/CE, y de hecho el 24 de octubre de 1998 venció el plazo previsto en dicha norma comunitaria.[147]

3.- Francia

Normas Constitucionales:

La Declaración de los Derechos del Hombre y del Ciudadano de 1789, en su artículo undécimo señala que:

"Artículo 11.: La libertad de comunicación de pensamiento y de comunicación es uno de los derechos más preciosos del hombre; todo ciudadano puede por lo tanto hablar, escribir, imprimir libremente, salvo aquellos casos en que se deba responder por abuso de esta libertad ante la ley".[148]

Aún cuando este artículo no reconoce expresamente la protección del derecho a la vida privada, sí puede interpretarse que los *abusos* de la libertad de expresión amenazan la intimidad de las personas.

---

[146] Información obtenida en el artículo "Privacy Laws & Business International Data Protection Roundup", de la revista la revista Privacy Laws&Bussines, International Newsletter, N° 60, de edición de enero del 2002, pág. 15.

[147] En virtud de lo resuelto por el Tribunal de Justicia de las Comunidades Europeas en el caso *Marleasing* (del 13-11-90, C-106/89), las personas pueden invocar las disposiciones de la Directiva ante sus tribunales nacionales. Además, las personas que se perjudiquen por la falta de implementación de la Directiva tendrán derecho a obtener una reparación ante los tribunales nacionales, de acuerdo a lo que el mismo Tribunal resolvió en el caso *Francovich* (sentencia del 19-11-91, C-6/90 y C-9/90).

[148] Artículo 11 de la Declaración de los Derechos del Hombre y del Ciudadano de 1789, traducción libre.

La Constitución Gala, vigente desde 1958, no hace tampoco mención expresa a la protección de este derecho, el cual realmente se encuentra amparado por la normativa interna, como se verá a continuación.

Normas Internas:

Dentro de la doctrina francesa, se distingue particularmente entre la protección del *secreto a la vida privada* y la protección del *secreto a otros intereses morales*. La primera de ellas, que es la que nos interesa, atribuye su desarrollo a la ley y a la jurisprudencia de ese país, y concretamente ello se vio reflejado con la creación de la Ley N° 70-643 del 17 de julio de 1970 que creó el actual artículo 9 del Código Civil.[149]

En cuanto a la protección de datos, ésta se garantiza mediante la *Ley de Informática, Ficheros y Libertades* (Ley 78-17), aprobada el 6 de enero de 1978. Uno de los grandes alcance que presenta esta ley es que se preocupa ya concretamente de regular el manejo de la informática frente al uso de datos de carácter personal. Es así que en su artículo primero determina el objeto de la ley en comento:

"Artículo 1: la informática debe estar al servicio de cada ciudadano. Su desarrollo debe realizarse dentro del marco de la cooperación internacional y no debe menoscabar la identidad humana, los derechos del hombre, la vida privada ni las libertades individuales o públicas ."[150]

La ley contienen 4 regímenes distintos en cuento a la legitimidad y funcionamiento de banco de datos, a saber: a) tratamientos realizados por cuenta del Estado (art.15); b) tratamientos realizados por cuenta de otras personas: antes de entrar en funcionamiento, la Comisión debe haber dictaminado que satisfacen las exigencias legales (art. 16); c) tratamientos públicos o privados que no menoscaban manifiestamente la vida privada ni las libertades y d) tratamientos basados en el repertorio nacional de identificación de personas físicas.

Respecto de la información que se obtiene del interesado, hay que hacerle saber, al igual que en otros ordenamientos jurídicos europeos, el carácter obligatorio o facultativo de sus respuestas, las consecuencias de su negativa a contestar, bs destinatarios de sus datos y la existencia de un derecho de acceso y de rectificación (está liberada del cumplimiento de esta exigencia la recolección de la información necesaria para la constatación de infracciones), como lo consagra el artículo 27.

[149] Según Pierre Kaiser, la jurisprudencia francesa ha reconocido primeramente el *derecho al secreto de las cartas confidenciales* y *el derecho de la persona sobre su imagen*. La consecución de estos dos derechos será un pilar fundamental de lo que ahora se entiende por *el derecho general al respeto de la vida privada*.

[150] Artículo 1 de la Ley de Informática, Ficheros y Libertades, o Ley 78-17, aprobada el 6 de enero de 1978.

Dentro de las medidas de seguridad que se establecen, el responsable del tratamiento debe adoptar todas las precauciones útiles para preservar la seguridad de los datos, particularmente para impedir que se distorsionen, deterioren o comuniquen a terceros no autorizados (art. 29).

Sobre la transmisión de datos al extranjero, al igual que en la generalidad de los países europeos, es necesaria una previa fiscalización y en virtud de ello esta ley establece que:

"Artículo 24. Según las modalidades fijadas por decreto del Consejo de Estado para asegurar el respeto a los principios establecidos en esta ley, y a propuesta o después de oír a la Comisión, esta transmisión puede estar sujeta a una autorización previa o reglamentación ."[151]

El ente encargado de velar por el adecuado cumplimiento de estas normas es la *Autoridad de Contralor*. Ella se conforma por la Comisión Nacional de Informática y de las Libertades (Comisión), autoridad administrativa independiente, compuesta por 17 miembros que permanecen 5 años en su cargo: 2 diputados y 2 senadores, 2 miembros del Consejo Económico y Social; 2 miembros o ex miembros del Consejo de Estado, 2 de la Corte de Casación, 2 del Tribunal de Cuentas; 2 personalidades calificadas por su conocimiento de las aplicaciones de la informática, nombradas por decreto a propuesta, respectivamente, del presidente de la Asamblea Nacional y del presidente del Senado, y 3 elegidas en razón de su autoridad y competencia, por decreto en Consejo de Ministros (art. 8). Una de las grandes particularidades de este órgano controlador es que tiene gran cantidad de miembros, pertenecientes a diversos organismos de la sociedad. Esto, desde mi punto de vista, es bastante favorable en cuanto se considerarían diversos factores a la hora de determinar una adecuada fiscalización del actuar de quienes se dedican al tratamiento de datos personales.

La vigilancia electrónica está regulada, por su parte, a través de la ley 91-636, del 10 de julio de 1991, relativa al secreto de la correspondencia emitida por vía de las telecomunicaciones. Esta norma fue creada por la Comisión Nacional de Control de las Intercepciones a la Seguridad, que establece reglas y controla anualmente las intercepciones telefónicas.[152] De acuerdo a este cuerpo legal, se justifica solamente la intercepción telefónica a través de una autorización judicial. Por consiguiente, debería ampararse igualmente a la correspondencia electrónica, que en definitiva también constituye una intercepción por vía de las telecomunicaciones.

---

[151] Artículo 1 de la Ley de Informática, Ficheros y Libertades, o Ley 78-17, aprobada el 6 de enero de 1978.

[152] La Corte Europea de Derechos Humanos ha condenado en varios casos a Francia por violación al art. 8 de la Convención Europea de Derechos Humanos, y la decisión que en 1990 tomó en el caso *Kruslin v. France* (caso 176-A, Serie A), dio lugar a la aprobación de la ley de 1991. Citado por Mercedes URIOSTE en Protección de Datos Personales, de Revista de la Secretaría de Derecho Comparado de la Corte Suprema de la Nación Argentina, pág. 94 de texto publicado en http://comunidad.derecho.org/redi/Habeas6.zip, visitada en febrero de 2002.

A fin de facilitar la aplicación de la ley a Internet, uno de los subcomités de la Comisión elaboró un modelo estándar para regular los procesos usados en los *sites*[153] de los ministerios. Este modelo, según la explicación de Mercedes Urioste, junto con la guía distribuida a los responsables de los *sites*, repite las recomendaciones elaboradas en cooperación con las personas comprometidas, relativas a los principales usos del Internet, a los mensajes electrónicos, a los foros de discusión, a la recolección electrónica de datos y a la difusión de información personal. En relación a este último aspecto, el subcomité, por un lado, destacó particularmente el derecho de los interesados a objetar de antemano o posteriormente la difusión de sus datos personales, y, por el otro, recordó a los usuarios de los *sites* la prohibición de usar los datos distribuidos de este modo con otros objetivos, en particular para fines comerciales.

Por lo tanto, en Francia, a la fecha de la elaboración del mencionado Informe, se habían reconocido los siguientes derechos: a) el derecho de las personas a objetar que las administraciones públicas difundan sus organigramas a través de *sites* o directorios públicos (decisión del 16-5-97, adoptada por el Primer Ministro en ejercicio de las facultades que le otorga el art. 15 de esta ley, publicada en el JO del 18-5-97); b) el derecho de los abonados que figuran en una guía de teléfonos a objetar su aparición en otras accesibles por Internet (recomendación de la Comisión del 8-7-98, OJ del 2-8-97, y decisión de France Telecom del 23-1-98 publicada en OJ de febrero de 1998).

Existen otras leyes específicas para documentos administrativos (ley 78-753, del 17 de julio de 1978, que contiene diversas medidas para mejorar las relaciones entre el público y la administración, y de orden público administrativo, social y fiscal), archivos (ley 79-18, del 3 de enero de 1979), vigilancia por video (ley de orientación y programación 95-73, del 21 de enero de 1995, relativa a la seguridad), y empleo (ley 92-1446, del 31 de diciembre de 1992, relativa al empleo y al desarrollo del empleo a tiempo parcial).

Desde este punto de vista, la legislación francesa ha sido pionera a nivel europeo en cuanto a regular el uso de Internet frente a la amenaza que representa respecto de la protección de la vida privada de sus ciudadanos, principalmente a nivel de la correspondencia electrónica.

Sin embargo, es precios recalcar que Francia aún no ha aprobado una nueva ley de protección de datos que se conforme a la Directiva 95/46/CE. [154]

[153] Se entiende por *site* al "punto de la red con dirección única y al que pueden acceder los usuarios para obtener información". Definición obtenida de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[154] Al igual que lo que señalábamos del caso alemán, en virtud de lo resuelto por el Tribunal de Justicia de las Comunidades Europeas en el caso *Marleasing* (del 13-11-90, caso C-106/89), las personas pueden invocar las disposiciones de la Directiva ante sus tribunales nacionales. Además, las personas que se perjudiquen por la falta de implementación de la Directiva tendrán derecho a obtener una reparación ante los tribunales nacionales, de acuerdo a lo que el mismo Tribunal resolvió en el caso *Francovich* (sentencia del 19-11-91, C-6/90 y C-9/90).

4.- Reino Unido

Normas Constitucionales:

Dentro de la Constitución inglesa no existen normas que protejan específicamente el derecho a la vida privada de las personas, menos sobre la protección de datos personales. Es en su derecho interno donde se resguardan estos derechos.

Normas de derecho interno:

La Ley de Protección de Datos o *Data Protection Act* de 1998, aprobada para adecuar la legislación británica a la Directiva 95/48 de la Comunidad Europea, entró en vigencia el primero de marzo del 2000 para todos los ficheros automáticos de datos y, gradualmente, para los ficheros manuales. Es un reemplazo de la anterior Ley de Protección de Datos de 1984. En virtud de ello, cualquier empresa que opere en Gran Bretaña y que maneje o almacene información sobre individuos (sean empleados, clientes o de cualquier otra índole) se verá afectada por los cambios introducidos por esta Ley. Si bien establece los rasgos esenciales del nuevo régimen, el Reino Unido debe dictar legislación complementaria para cumplir adecuadamente con la Directiva.

Esta ley, en su Sección 1.1 prevé dos figuras especiales: el *Controlador de los Datos* (Controlador) y el *Procesador de los Datos* (Procesador). El Controlador es la persona que sola, conjuntamente, o en común con otras personas, determina los objetivos y forma del procesamiento de los datos personales.
El Procesador es cualquier persona no empleada del Controlador, que procesa los datos en nombre de éste.

Es curioso que se defina de una manera tan amplia al titular de la protección de datos como "*toda persona de existencia visible*" (Sección 1.1). De acuerdo a la interpretación de la definición, debería contener a las personas jurídicas, ya que al ser creadas existen, y la visibilidad de su existencia se acredita a través de los documentos que dan fe de su nacimiento a la vida del derecho .

Esta ley establece determinados Principios de Protección de Datos, que en resumen corresponden a:

Primer Principio: los datos personales deben ser procesados lícitamente y de buena fe y, en especial, no deben ser procesados salvo que se cumpla, al menos, una de las condiciones del Segundo Anexo (§ 1 del Primer Anexo)[155].

[155] Son condiciones del Segundo Anexo: a) que el interesado haya dado su consentimiento; b) que el procesamiento sea necesario: b') para el cumplimiento de un contrato en el que el interesado es parte, o para implementar medidas precontractuales en respuesta a una solicitud del interesado, o para cumplir alguna obligación legal de naturaleza no contractual del Controlador, o para proteger los intereses vitales del interesado; b'') para la administración de justicia, o para que una persona, la Corona, un Ministro de la Corona o un departamento gubernamental cumplan una obligación jurídica; b''') para proteger los intereses legítimos del Controlador o del tercero a quien los datos se transmiten, excepto

Segundo Principio: los datos personales sólo deben ser procesados para uno o más objetivos específicos y lícitos, y no deben ser ulteriormente procesados en forma incompatible con dichos objetivos (§ 2 de la Parte I del Primer Anexo).
Tercer Principio: los datos personales deben ser adecuados, relevantes y no excesivos en relación a los fines del procesamiento (§ 3 de la Parte I del Primer Anexo).
Cuarto Principio: los datos personales deben ser exactos y, cuando sea necesario, actualizados (§ 4 de la Parte I del Primer Anexo).[156]
Quinto Principio: los datos personales sólo deben conservarse durante el tiempo necesario para cumplir el propósito que justificó su recolección (§ 5 de la Parte I del Primer Anexo).
Sexto Principio: los datos personales deben procesarse respetando los derechos que esta ley acuerda a los interesados (§ 6 de la Parte I del Primer Anexo).[157]

En cuanto a la transmisión de datos al extranjero, según el Octavo Principio, los datos personales no pueden transmitirse a un país o territorio fuera de la Comunidad Europea que no brinde un adecuado nivel de protección a los derechos y libertades de los interesados en relación al procesamiento de datos personales (§ 8 de la Parte I del Primer Anexo). A este respecto la ley define lo que debe entenderse como nivel de protección adecuado:

"§ 13 de la Parte II del Primer Anexo: (...) como el que es adecuado en todas las circunstancias del caso, teniendo particularmente en cuenta la naturaleza de los datos personales, los países o territorios de origen y de destino de los datos, los objetivos y el plazo del procesamiento, el derecho vigente en el país o territorio en cuestión y las obligaciones internacionales que éste ha asumido, y cualquier código de conducta relevante u otras reglas que sean ejecutables en dicho país o territorio (generales o establecidas por vía contractual para casos determinados) y toda medida de seguridad adoptada en relación a los datos en ese país o territorio ."[158]

Esta Ley también ha establecido las llamadas *Autoridades de Contralor*, representadas por el Comisionado de Protección de Datos (Comisionado) y el Tribunal de la Protección de Datos (Tribunal).

---

cuando el procesamiento es improcedente, en un caso determinado, porque sus derechos y libertades o intereses legítimos del interesado, aun cuando el Secretario de Estado puede dictar una orden estableciendo los supuestos en que esta condición se considera satisfecha o no (Segundo Anexo).

[156] A este respecto, la Parte II de este mismo Anexo dispone que este principio no debe considerarse violado por cualquier error en los datos personales que reflejan con precisión la información que el Controlador obtuvo del interesado o de un tercero cuando: a) teniendo en cuenta el objetivo de la recolección y posterior procesamiento, el Controlador ha seguido los pasos razonables para asegurar su exactitud; y b) en su caso, contienen constancia de que el interesado ha notificado al Controlador su opinión de que son inexactos (§ 7).

[157] La Parte II de este mismo Anexo dispone que se considera que un Controlador viola este principio si y sólo si: a) no permite el derecho de acceso; b) no hace lugar a una solicitud de no comenzar o dejar de procesar datos personales de una persona que legítimamente así se lo solicita con base en el perjuicio que el procesamiento le produce, u omite notificar dicha negativa; c) no accede a una solicitud de no comenzar o dejar de procesar datos personales con fines de *marketing* directo, de una persona que así se lo solicita; o d) no accede a una solicitud de que se asegure de que no se están adoptando decisiones automatizadas relativas a su persona (§ 8).
[158] Ley de Protección de Datos del Reino Unido, § 13 de la Parte II del Primer Anexo.

a) Comisionado: esta figura ya existía en la ley de 1984 bajo el nombre de Registrador de Protección de datos. La ley, en el Quinto Anexo, dispone expresamente que ni el Comisionado ni sus funcionarios y personal, deben considerarse empleados o agentes de la Corona (§ 1.2).

b) Tribunal: sus miembros permanecen en el cargo durante el período que se fije en su designación y son reelegibles (Sec. 12.1). En cualquier momento pueden renunciar, con notificación por escrito al Lord Chancellor (en caso del Presidente o del Vicepresidente) o al Secretario de Estado (los demás miembros) (Sec. 12.2).

Urioste señala que con respecto al derecho de la vida privada de las personas dentro de las comunicaciones electrónicas, Gran Bretaña ha creado una de las mayores controversias existentes hasta la fecha. La *Ley de Poderes Investigativos*, aprobada por la Cámara de los Comunes el 26 de julio de 2000 y entrada en vigencia en noviembre del mismo año fue diseñada para perseguir a los criminales y pedofílicos en Internet. Esta ley esquematiza el procedimiento que debe seguir la policía británica para la obtención de órdenes judiciales que les autoricen a interceptar el correo electrónico y el historial de navegación por Internet de un sospechoso. Para lograr tal intercepción, el gobierno británico pretende instalar "cajas negras" en cada PSI .[159]

La controversia comenzó desde el momento en que los servicios de inteligencia ingleses hicieron una petición para que se cambiara la legislación de ese país sobre protección de datos. En su petición, la inteligencia inglesa solicitó plenos poderes a la hora de tener acceso a las llamadas, correos electrónicos y conexiones a Internet de los ciudadanos ingleses. La solicitud fue formalizada en un informe redactado por el Director General del Servicio Nacional de Inteligencia Criminal, en el cual se señala que:

"Los datos de las comunicaciones individuales deben ser retenidos en interés de la justicia, para preservar y proteger los mismos como evidencias para establecer pruebas en la inocencia o culpabilidad."[160]

Los líderes del Grupo de Ingenieros de Internet se reunieron para discutir si la Ley de Poderes Investigativos aprobada por Gran Bretaña implica un riesgo a la intimidad inaceptable para sus miembros. En opinión de Urioste, la ley también ha sido criticada por los PSI británicos y por las empresas del campo de la tecnología de la información, puesto que consideran que la Ley, irónicamente llamada RIP por los ingleses[161], facilita demasiado las posibilidades de obtención de la orden judicial necesaria para intervenir cualquier correo electrónico o historial de navegación.

---

[159] Ver nota 34 definición de ISP.

[160] Citado por Alexander ROSEMBERG HOLCBLAT y Moirah SÁNCHEZ SAN en El derecho a la privacidad en internte, pág. 37, refiriéndose a texto publicado en http://vlex.com/es/actualidad/articulos/3439.

[161] RIP en inglés es el acrónimo de Rest In Peace, que significa "descanse en paz".

Finalmente, cabe destacar que la Ley de Poderes Investigativos establece también, en su Sección 4, que cualquier intercepción de una comunicación durante su período de transmisión por medio de sistemas de telecomunicaciones será autorizada si tal intercepción se realiza con el propósito de obtener información sobre las comunicaciones de una persona que se encuentre fuera del territorio de Gran Bretaña, o que, al menos, el interceptor tenga buenas razones para pensar que el sujeto se encuentra fuera de dicho territorio.

5.- España

Normas Constitucionales:

La Constitución española es una de las pocas Cartas Políticas que consagra expresamente la protección del derecho a la vida privada de las personas frente al uso de la informática, lo cual se ve reflejado en su artículo décimo octavo que consagra que:

"Artículo 18.-

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."[162]

De la interpretación de esta norma claramente se desprende el amparo que el ordenamiento jurídico otorga a las amenazas producidas por el uso de la informática a través de Internet. De ello se puede desprender una conclusión sumamente importante: el derecho a la vida íntima de las personas frente a las amenazas que provoca Internet tiene expresamente un resguardo constitucional.

Normas Internas:

Los españoles, en cuanto al tratamiento de datos de carácter personal se rigen en la actualidad por la Ley Orgánica 15/99 del 13 de diciembre de 1999, también conocida como la LOPD (Ley Orgánica de Protección de Datos), que según el artículo derogatorio de la misma[163], reemplazó a la antigua LORTAD (Ley Orgánica de Regulación de Tratamiento Automatizado de Datos) de 1992.

[162] Constitución Española aprobada por las Cortes en Sesiones Plenarias del Congreso de los Diputados y del Senado. 31 de Octubre de 1978. Ratificada por el Pueblo Español en Referéndum de 6 de Diciembre de 1978. Sancionada por S.M. el Rey ante las Cortes el 27 de Diciembre de 1978. Reformada el 27 de Agosto de 1992.

[163] La disposición derogatoria única de la Ley 15/99 establece que: "Queda derogada la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal".

Según el artículo primero de la LOPD, el objetivo de la misma es el siguiente:

"Artículo 1. *Objeto.*

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar."[164]

Según este mismo cuerpo legal, los interesados a los que se soliciten datos personales deberán ser previamente informados de modo *expreso, preciso e inequívoco* como lo señala es propio artículo quinto. Ello representa una eventual garantía frente a la invasión de la vida privada de las personas de manera arbitraria.

Resulta interesante también mencionar el artículo 7 de esta Ley en cuanto menciona a los datos "especialmente protegidos", lo cual representa una ampliación de lo que en muchas legislaciones se conocen como "datos sensibles":

"Artículo 7. *Datos especialmente protegidos*

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

[164] Artículo 1 de la Ley 13/99 sobre Protección de Datos de Carácter Personal de España.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

6. No obstante lo dispuesto en los apartados anteriores podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto".

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento."[165]

Así mismo, al igual que otros países de Europa, España también ha adoptado los llamados "Códigos de Conducta" o "Códigos Tipo", que según el artículo 32, "tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas".

En cuanto a la transmisión de datos de carácter personal a terceros países, estos no podrán realizarse a países que no presten un nivel de protección equiparable a esta Ley(art. 33).[166]

La protección de datos personales se encuentra protegida en España a través de la Agencia Protectora de Datos (Agencia), descrita en el artículo 35:

"Artículo 35. *Naturaleza y régimen jurídico.*

1. La Agencia de Protección de Datos es un Ente de Derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno".[167]

---

[165] Artículo 1 de la Ley 13/99 sobre Protección de Datos de Carácter Personal de España.

[166] Según el artículo 33 en su segundo punto, "El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos de finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".

[167] Artículo 35 de la Ley 13/99 sobre Protección de Datos de Carácter Personal de España

Así mismo, existe el Registro General de Protección de Datos (RGPD) es el órgano de la Agencia de Protección de Datos al que corresponde velar por la publicidad de la existencia de los ficheros de datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de información, oposición, acceso, rectificación y cancelación de datos (art. 39).

Aparte de esta ley, existen otras normativas tendientes a perfeccionar la aplicación de la LOPD para proteger la vida privada de las personas. Dentro de ellas está el Real Decreto 1332/94 de 20 de junio por el que se desarrollan algunos preceptos de la Ley Orgánica; el Real Decreto 994/1999 de 11 de junio por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal y el Real Decreto 195/2000 de 11 de febrero por el que se establece el plazo para implementar las Medidas de Seguridad de los Ficheros Automatizados previstas por el Reglamento aprobado por el Real Decreto 994/1999 antes mencionado.

En la actualidad, existe un anteproyecto de la Ley de Servicios de la Sociedad de la Información (LSSI) que pretende regular las actividades económicas en Internet. Así, establece, según las pautas dictadas por la Unión Europea, una serie de normas para las *webs*[168] de comercio electrónico e incluye una regulación acerca del "Spam" [169] (hasta ahora, el aspecto más difundido de la nueva ley), que según la doctrina, es una de las maneras más usuales de atentar contra el derecho a la vida privada de las personas a través de Internet, y que de concretarse tal proyecto, sería un avance notable en esta lucha. Sin embargo, el artículo primero de dicha norma claramente señala que no regulará la protección de datos personales.[170] Ya en la actualidad esta ley ha despertado mucha polémica en cuanto a su aplicación y aún cuando está próxima a entrar en vigencia, sin duda alguna que va a marcar una pauta en cuanto a la regulación de Internet.

---

[168] Se entiende por *web* o *página web* al "Fichero (o archivo) que constituye una unidad significativa de información accesible en la WWW a través de un programa navegador. Su contenido puede ir desde un texto corto a un voluminoso conjunto de textos, gráficos estáticos o en movimiento, sonido, etc. El término página web se utiliza a veces, a entender del autor de forma incorrecta, para designar el contenido global de un sitio web, cuando en ese caso debería decirse páginas web o sitio web." Definición obtenida de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo de 2002. Según la doctrina.

[169] Se entiende por *Spam* al "envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico. Literalmente quiere decir loncha de mortadela", según definición obtenida de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo de 2002.

[170] El Anteproyecto de ley de servicios de la sociedad de la información y de comercio electrónico, en el Título I sobre Disposiciones Generales, el Capítulo I se refiere a la finalidad y conceptos básicos señalando que: "Artículo 1. Objeto. 1. Esta Ley regula ciertos aspectos jurídicos de los servicios de la sociedad de la información y de la contratación por vía electrónica, como las obligaciones de los prestadores de servicios que actúan como intermediarios en la transmisión de contenidos por la Red, las comunicaciones comerciales, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.2. Las disposiciones contenidas en esta Ley no afectarán a la aplicación de la normativa existente sobre protección de la salud pública, datos personales y derechos de los consumidores y usuarios, a las materias reguladas por la misma." Información obtenida en www.agenciaprotecciondatos.org, visitada en marzo de 2002. Recomiendo consultar también el texto de este proyecto de ley en http://www.libertaddigital.com/suplementos/pdf/anteproyecto_lssice.pdf.

América del Norte

1.- Estados Unidos de América:

Normas Constitucionales:

La Constitución norteamericana no contiene ninguna disposición expresa que proteja este derecho. Sin embargo, ya hemos visto cómo, a partir de la IV y V Enmiendas fue desarrollado este derecho tanto por la doctrina como por la jurisprudencia. En todo caso, las disposiciones constitucionales más importantes en materia de protección a la llamada "privacy" son la IV y V Enmiendas, que son del tenor siguiente:

"IV Enmienda.- El derecho de los individuos a estar protegidos en contra de búsquedas no razonables en su persona, casa, documentos y efectos personales no será violentado. Ninguna orden judicial podrá ser emitida sin causa probable apoyada por declaración jurada, y deberá describir expresamente el lugar a ser registrado y las personas que serán detenidas."

"V Enmienda.- Ninguna persona… será compelida en ningún caso criminal, a ser testigo contra si mismo"[171]

Como lo señalan Rosemberg y Sánchez Sánz, "el legislador estadounidense separó las obligaciones del Estado de las obligaciones de los particulares con respecto a la observancia del derecho a la privacidad. Así, la Corte Suprema de los Estados Unidos ha reconocido el derecho a la privacidad basado en la Constitución, pero este derecho sólo es aplicable al a protección del derecho a la privacidad contra las injerencias del gobierno, y no es extensible al ámbito privado". [172]

Normas de Derecho Interno

Al igual que dentro del ámbito constitucional, en el derecho interno norteamericano existe también una distinción entre la protección del derecho a la intimidad del sector público y la del sector privado.

.

En el sector público, una de las leyes más importantes es la *Privacy Act* de 1974. Esta Ley regula la forma en que el gobierno federal recolecta y utiliza los datos personales contenidos en sus bases de datos. Según esta Ley, los sujetos de los datos tienen el derecho de acceder a la información personal que de ellos mantenga el gobierno, y de solicitar que cualquier información inexacta sea corregida.

---

[171] Enmiendas IV y V de la Constitución de los Estados Unidos de América.

[172] Alexander ROSEMBERG HOLCBLAT y Moirah SÁNCHEZ SANZ, El derecho a la privacidad en internte, pág. 37 de texto publicado en http://vlex.com/redi/No._37_-_Agosto_del_2001/5, visitado en enero de 2002

Para Rosemberg y Sánchez Sánz, "la Privacy Act busca proveer a los ciudadanos americanos con un cierto nivel de control sobre la información que de ellos posee el gobierno, y prohíbe a los organismos públicos la revelación o diseminación de datos personales sin el consentimiento del sujeto de los datos. Sin embargo, la Ley contiene numerosas excepciones que permiten al gobierno estadounidense el uso y revelación de datos sin consentimiento, aunque el principio general implica el reconocimiento de que los individuos tienen ciertos derechos con respecto a sus datos personales".[173]

Es preciso recalcar que dentro del sistema norteamericano existe una fuerte tendencia a que las normas de Internet se guíen a través de la autorregulación, ello incluso apoyado en su momento por el ex presidente Bill Clinton. Sin embargo, en la actualidad el Congreso de los Estados Unidos está discutiendo más de un proyecto de ley sobre privacidad hoy en día.[174]

Una de las normas más importantes en cuanto a la protección del derecho a la vida privada en Internet es la Ley de Privacidad de las Comunicaciones Electrónicas, o *ECPA* según sus siglas en inglés, vigente a partir del año 2000, la cual protege todas las formas de comunicación electrónica, incluyendo la comunicación telefónica de voz y las comunicaciones digitales de computadora a computadora como el correo electrónico y los mensajes almacenados en boletines electrónicos.

Según Thomas J. Smedinghoff, el Senado estadounidense expresó que el objeto de la ECPA es regular "el creciente problema del acceso y uso, por personas no autorizadas, a las comunicaciones electrónicas que no deben estar disponibles al público"[175]

Uno de los aspectos novedosos de la ECPA es que sus provisiones son aplicables tanto al sector público como al privado. Los dos elementos claves regulados por dicha Ley son:

1) la intercepción y revelación de las comunicaciones electrónicas, y
2) el acceso ilegal a las comunicaciones electrónicas almacenadas en computadoras.

---

[173] Ibídem, pág. 40.

[174]Según Rosemberg y Sánchez Sanz, "las dos áreas que cuentan con regulación específica sobre la protección del derecho a la privacidad en los Estados Unidos hoy en día son el área laboral y la de los menores. En cuanto al aspecto laboral, la situación representa un estado de tensión único entre el interés de los empleadores en mantener operaciones eficientes y el derecho de los empleados a que se les respete su privacidad. En tiempos previos a la intervención del Congreso en la materia, los empleados solían exigir la protección de sus intereses privados por medio de demandas de *common law*, tales como las que denuncian invasión a la privacidad o perturbación emocional intencional. La Ley de Privacidad de las Comunicaciones Electrónicas de 1986 proscribió la intercepción intencional de las comunicaciones electrónicas sin el consentimiento del sujeto pasivo, al igual su uso o revelación por medios orales, escritos o electrónicos". Ver pág. 39 de texto publicado en http://vlex.com/redi/No._37_-_Agosto_del_2001/5, visitado en enero de 2002

[175] Thomas J. SMDINGHOFF, On-line Law.Addison-Wesley Developers Press. 5ta Reimpresión. EEUU, 2000, citado por Alexander ROSEMBERG HOLCBLAT y Moirah SÁNCHEZ SANZ, El derecho a la privacidad en internte, pág. 40 de texto publicado en http://vlex.com/redi/No._37_-_Agosto_del_2001/5, visitado en enero de 2002.

La prohibición de interceptar intencionalmente una comunicación electrónica y de revelar su contenido es aplicable no sólo para quienes buscan irrumpir en un sistema de comunicaciones electrónicas, como los llamados *hackers*[176], sino para los propietarios y operadores de esos sistemas, como los PSI, los administradores de redes privadas, los operadores de sistemas de los boletines en línea, y otros. Sin embargo, dicha restricción no prohíbe a los empleados o agentes de servicios de comunicación electrónica la intercepción, uso y revelación de tales comunicaciones, siempre que estén dentro del curso normal de las actividades inherentes a la prestación del servicio, o la intercepción, uso o revelación obedezcan a la protección de los intereses del proveedor del servicio. Aunque pareciera bastante simple, tiene implicaciones significativas en el ámbito del monitoreo de correos electrónicos de empleados por parte de las empresas que los emplean.

Sin embargo, la ECPA no contiene ninguna disposición respecto del derecho a la vida privada de los usuarios contra los operadores de sistemas de comunicación electrónica, lo cual también es significativo a la luz del problema del monitoreo de e-mails de empleados por las empresas, tema este último de los más debatidos y discutidos respecto de esta Ley.

Otra de las normas más trascendentales del ordenamiento jurídico norteamericano referente a la regulación de la red es la COPPA, la cual fue aprobada en 1998, y entró en vigencia el 21 de abril de 2000. Se trata de la primera ley estadounidense aplicable a la privacidad de los datos personales en Internet. Su ámbito de aplicación es sin embargo bastante restringido ya que la Ley solamente regula la recolección, utilización y revelación de datos personales en línea de niños menores de 13 años. Se establece de esta manera requerimientos muy específicos respecto del uso, la notificación, el consentimiento de los padres, y la posibilidad de revisar y bloquear los datos recolectados de los menores.

Merecen ser mencionados dentro de la normativa de la COPPA algunos puntos entre ellos lo referente a la notificación. Ella se traduce en dos elementos relativos las páginas web[177], las cuales deben:

1) publicar en-línea una declaración de sus políticas de privacidad; y

2) emitir una notificación a los padres en la que describa cuáles son los datos personales del niño que está recolectando, cómo funciona la recolección, cómo pretende utilizarla, y cuáles son las políticas de la página con respecto a la revelación de tal información.

[176] Se entiende por *hacker* o pirata a " Una persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de un ordenador o de una red de ordenadores. Este término se suele utilizar indebidamente como peyorativo, cuando en este último sentido sería más correcto utilizar el término *cracker*. Los *hackers* proclaman tener una ética y unos principios contestatarios e inconformistas pero no delictivos". Definición obtenida de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo de 2002. Según la doctrina.

[177] Ver definición de página web en nota 55.

Por otra parte, las páginas web que manejan datos personales de niños deben obtener el consentimiento expreso y verificable antes de recolectar, utilizar o revelar tales datos. Además, debe otorgarse a los padres oportunidad suficiente para revisar los datos personales recolectados de sus hijos, para solicitar que sean borrados, y para prohibir su uso y revelación.

En cuarto lugar, la COPPA prohíbe que los controladores de estos datos condicionen la participación del niño actividades en línea a la revelación de información más allá de la estrictamente necesaria para que se produzca tal participación. Finalmente, la COPPA exige que se establezcan y mantengan procedimientos razonables para proteger la confidencialidad, seguridad e integridad de los datos personales.

A modo de conclusión se puede decir que las leyes estadounidenses que regulan el derecho a la intimidad son complementadas por las normas internas de cada industria, y ésa ha sido la tendencia tradicional. Las empresas y asociaciones han desarrollado, adoptado y publicado sus propias políticas de protección de datos personales y comunicaciones electrónicas. Esta mezcla de leyes federales y autorregulación difiere en gran medida de las políticas regulatorias adoptadas en el resto del mundo, en especial de las europeas.

América Latina

La mayoría de los países latinoamericanos reconocen dentro de sus Cartas Fundamentales el derecho a la protección de la vida privada de las personas como un derecho de carácter fundamental. Sin lugar a dudas que éste derecho también ha ido evolucionando en nuestros ordenamientos jurídicos, aún cuando tal evolución ha sido lenta y engorrosa. Dentro de este progreso debe considerarse la inclusión de normas relativas a la protección de datos de carácter personal y conjuntamente con ellas la acción o recurso de habeas data.

Recogiendo palabras de Oscar Puccinelli, "El retraso de estas sociedades a la tecnología informática ha provocado que las normas sobre protección de datos personales hayan demorado en dictarse, y sean aún bien escasas. Como bien fuera indicado, durante varios años las leyes de protección de datos fueron consideradas como un "lujo democrático para países ricos" por los países en desarrollo, razón por la cual, según informa CORREA, solo hasta 1988 Argentina, Colombia y Chile se encontraban diseñando proyectos al respecto".[178]

El mismo autor, refiriéndose a los antecedentes del habeas data en nuestros países señala que: "El *habeas data* indoiberoamericano presenta dos versiones principales: una dedicada a la tutela de ciertos derechos a la protección de los datos personales (*habeas data* propio o tradicional), y la otra, preocupada por garantizar el derecho de acceso a la información pública (*habeas data* impropio). La primera de ellas, generalmente

[178] Oscar PUCCINELLI, El Habeas Data en Indoiberoamérica, pág. 191, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1999.

reconocida en la doctrina y la jurisprudencia como *habeas data*; y la segunda, ordinariamente no vinculada con esta nueva garantía , a excepción de la Constitución peruana que si lo hace".[179]

Desde esta perspectiva, ha continuación se hará un breve estudio de las legislaciones y de la normativa interna de ciertos países latinoamericanos, dedicadas a la protección del derecho a la intimidad y del reconocimiento jurídico al ya mencionado habeas data, que en general tienen un desarrollo bastante más precarios que el de los países recién estudiados.

1.- Brasil

Normas Constitucionales:

La Constitución Federal del Brasil, promulgada en el año de 1988, protege constitucionalmente el derecho a la vida privada de sus ciudadanos. Tal protección se encuentra consagrada en los siguientes artículos:

"Artículo 5, X.- La privacidad, vida privada, honor e imagen de las personas son inviolables. Se asegura el derecho a la compensación por daño material o moral que resulte de las violaciones a este derecho.

Artículo 5, XII.- El secreto de la correspondencia y de las comunicaciones telegráficas, de datos y telefónicas es inviolable, excepto mediante orden de un tribunal y bajo las circunstancias y en la forma que prescribe la ley para propósitos de investigación criminal o presentación de pruebas en juicio."[180]

Cabe destacar que el ordenamiento jurídico brasilero es uno de los pioneros a nivel latinoamericano en introducir el recurso de Habeas Data dentro de su Carta Fundamental. Es así que se señala que:

"Artículo 5, LXXII. Se concederá *habeas data*:
a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante, que consten en registros o bancos de datos de entidades gubernamentales o de carácter público;[181]
b) para rectificar datos, cuando no de prefiera hacerlo por procedimiento secreto, judicial o administrativo".[182]

---

[179] Ibídem, pág. 194. Ver de este mismo autor el estudio minucioso que hace del recurso de habeas data, su evolución, clasificación y distintas conceptualizaciones.

[180] Artículo 5,X y XII de la Constitución de la República de Brasil.

[181] Artículo 5,LXXII de la Constitución de la República de Brasil. Dentro de la doctrina brasilera, al utilizarse la expresión "a la persona del impetrante" en el artículo recién citado, existe un debate sobre si el recurso de habeas data ampara o no a las personas jurídicas. Me parece acertada la opinión de Alexandre de Moraes, quien señala que "el *habeas data* podrá ser utilizado tanto por persona física (brasileña o extranjera) como por persona jurídica, pues en relación con esas, tiene derecho a la correcta identificación propia en el mundo social". Citado por Oscar PUCCINELLI, El Habeas Data en Indoiberoamérica, pág. 307, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1999.

[182]Constitución de la República de Brasil. En: Constituciones del Mundo. http://www.cepc.es, visitado en marzo de 2002.

Normas de Derecho Interno:

Si bien la Constitución Brasilera reconoce el habeas data, no serán sino sus normas internas las encargadas de regular la aplicación de este recurso de una manera más concreta, ya que como se desprende de los artículos recién citados, en el Código Político apenas se dejaron sentadas las bases del núcleo esencial de dicho recurso.

Desde esta perspectiva, será la ley 9.507 del 12 de noviembre de 1997 la encargada de regular el "derecho de acceso a informaciones" y el "rito procesal de habeas data". Así, el artículo séptimo de dicha ley señala los casos en que procede este remedio constitucional:

"Artículo 7. Concédese *habeas data*:

I. para asegurar informaciones relativas a la persona del impetrante, obrantes en registros o bancos de entidades gubernamentales o de carácter público;
II. para la rectificación de datos, cuando no se prefiera hacerlo por proceso sigiloso, judicial o administrativo.
III. para la anotación en los asientos del interesado, de contestación o explicación sobre dato verdadero pero justificable y que esté en pendencia judicial o amigable". [183]

Lo curioso de este artículo es el tercer numeral, donde Alexandre de Moraes hace notar una expansión del tradicional derecho de habeas data, refiriéndose a "la idea de evitar o remediar posibles humillaciones que pueda sufrir el individuo en virtud de datos constantes que, a pesar de ser verdaderos, serían insuficientes para un correcto y amplio análisis, posibilitando una interpretación dudosa o errónea, si no hubiere la posibilidad de mayores esclarecimientos". [184]

Por otra parte, está la Ley 9269/96, que trata sobre la vigilancia de las conversaciones telefónicas, y las comunicaciones informáticas y telemáticas, y establece que dicha vigilancia sólo será legal previa aprobación de un tribunal competente. Dentro de esta Ley resulta interesante mencionar el décimo artículo, el cual establece que:

"Artículo 10. La intercepción de una comunicación telefónica informática o telemática sin la debida autorización de un tribunal, o para propósitos no autorizados por ley constituye delito (....)".[185]

[183] Artículo 7 de la Ley 9.507 de 12 de noviembre de 1997 que regula el Recurso de Habeas Data en Brasil.

[184] Citado por por Oscar PUCCINELLI, El Habeas Data en Indoiberoamérica, pág. 307, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1999.

[185] Artículo 10 de Ley 9269 del año 1996 sobre Regulación de Comunicaciones.

Lo curioso de este artículo es que perfectamente se desprende respecto de la protección de las comunicaciones que se hacen vía Internet, como por ejemplo el correo electrónico, o de cualquier otra forma de comunicación que se haga a través de la utilización de la informática. Esto ha tenido mucha relevancia tanto en la doctrina como en la jurisprudencia brasilera en cuanto a la protección de la correspondencia en el ámbito laboral entre trabajadores y empleadores.

2.- Ecuador.

Noemas Constitucionales:

La Constitución Política de la República de Ecuador, aprobada en 1998, reconoce el derecho a la vida privada. Es así que en el Capítulo Segundo se consagran los Derechos Civiles, y refiriéndose a ellos el artículo 23 dispone que:

"Artículo 23.- Sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes:

8.- El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona.

9.- El derecho a la libertad de opinión y de expresión del pensamiento en todas sus formas, a través de cualquier medio de comunicación, sin perjuicio de las responsabilidades previstas en la ley. La persona afectada por afirmaciones sin pruebas o inexactas, o agraviada en su honra por informaciones o publicaciones no pagadas hechas por la prensa u otros medios de comunicación social, tendrá derecho a que estos hagan la rectificación correspondiente en forma obligatoria, inmediata y gratuita, y en el mismo espacio o tiempo de la información o publicación que se rectifica.

12.- La inviolabilidad de domicilio. Nadie podrá ingresar en él ni realizar inspecciones o registros sin la autorización de la persona que lo habita o sin orden judicial, en los casos y forma que establece la ley.

13.- La inviolabilidad y el secreto de la correspondencia. Esta sólo podrá ser retenida, abierta y examinada en los casos previstos en la ley. Se guardará el secreto de los asuntos ajenos al hecho que motive su examen. El mismo principio se observará con respecto a cualquier otro tipo o forma de comunicación."[186] (subrayado es mío).

Uno de los numerales más interesantes para el tema de estudio de este trabajo es el décimo tercero ya que reconoce el derecho al secreto en relación a las distintas formas de comunicación. Como se desprende del numeral recién mencionado, el legislador tuvo una visión futurista en cuanto protege el derecho a la inviolabilidad y secreto de las comunicaciones, cualquiera sea la forma o tipo en que se exprese. De ello se desprende que el secreto de las comunicaciones a través de Internet tienen protección de rango constitucional.

[186]Artículos 8 y 13 de la Constitución de la República del Ecuador, vigente desde 1998.

El habeas data también tiene un reconocimiento en el Código Político ecuatoriano, y es así que en el Capítulo Sexto, sección segunda, referente a las Garantías de los Derechos se hace alusión a este recurso. Tal artículo reza:

"Artículo 94.- Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito.

Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos.

Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización.

La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional".[187]

Normas internas:

Dentro de las normas internas está la Ley del Control Constitucional, promulgada en el Registro Oficial con fecha 2 de julio de 1997, en la cual está detallada la regulación de la acción de habeas data en el Ecuador.

Una de las particularidades de esta ley es que considera como sujeto activo tanto a personas naturales como jurídicas. Así lo dispone el artículo 34:

"Artículo 34.- Las personas naturales o jurídicas, nacionales o extranjeras, que deseen tener documentos, bancos de datos e informes que sobre sí mismas o sus bienes están en poder de entidades públicas, de personas naturales o jurídicas privadas, así como conocer el uso o finalidad que se les haya dado o se les esté por dar, podrán interponer el recurso de *habeas data* para requerir las respuestas y exigir el cumplimiento de las medidas tutelares prescritas en esta ley, por parte de personas que posean tales datos o informaciones".[188]

Otra de las particularidades del ordenamiento jurídico ecuatoriano es que se ha creado la figura del *Defensor del Pueblo*, ente destinado a velar por el cumplimiento de las garantías que establece la Constitución. Siguiendo las palabras del constitucionalista Hernán Salgado Pesantes, "el defensor del pueblo está

[187] Artículo 94 de la Constitución de la República del Ecuador, vigente desde 1998.

[188] Artículo 34 de la Ley de Control Constitucional, vigente desde el 2 de julio de 1997.

legitimado , por las reformas de 1996, para presentar ante el Tribunal Constitucional aquellos casos de denegación de los recursos de *habeas corpus*, de amparo o de *habeas data*".[189]

En cuanto a la protección del derecho a la vida privada en Internet, existe en la actualidad el "Proyecto de Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos", el cual se encuentra en discusión actualmente en el Congreso del Ecuador. Este Proyecto de Ley establece que:

"Artículo 11 (inciso tercero).- Los datos obtenidos con el consentimiento y voluntad de una persona responderán a los principios de privacidad e intimidad garantizados por la Constitución de la República y podrán ser utilizados o transferidos únicamente con su autorización u orden de autoridad competente."

"Artículo 42.- Privacidad: Como privacidad del usuario se entiende el derecho a la intimidad y el derecho a no recibir información directamente o mediante cadenas, el usuario deberá haber suscrito una autorización expresa al iniciador o emisor del mensaje de datos.
El usuario podrá solicitar en cualquier momento su exclusión de cadenas de mensajes o de bases de datos en las cuales conste inscrito. En caso de violarse el derecho a la privacidad, el usuario podrá iniciar las acciones que le concede la Ley y el iniciador o emisor del mensaje de datos será condenado al pago de la respectiva indemnización por daños y perjuicios."

Es particularmente destacable este proyecto de ley ya que pretende solucionar una serie de amenazas al derecho a la vida privada de las personas que traen consigo las nuevas tecnologías, como son los que presentan los PSI, el correo electrónico no deseado o *Spam*[190], y la protección de su correspondencia en línea, así como el reconocimiento de la responsabilidad extracontractual frente a la violación del derecho a la intimidad de las personas.

Sin embargo, aún cuando este artículo todavía es poco preciso desde mi punto de vista, sin duda alguna que se trata de un paso más en la labor del legislador por proteger los derechos que la Carta Fundamental reconoce frente a los avances de la Tecnología.

3.- Argentina:

Normas Constitucionales:

[189] Citado por Oscar PUCCINELLI, El Habeas Data en Indoiberoamérica, pág. 546, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1999.
[190] Ver definición de *Spam* en nota 57.

En cuanto al recurso de habeas data, éste se ha visto consagrado indirectamente en el artículo 43 de la Constitución Federal, la cual rige para todo el territorio argentino.[191]

"Artículo 43. Toda persona podrá interponer esta acción (se refiere a la de amparo) para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística". [192]

Dentro del sistema constitucional argentino, el habeas data se ha consagrado, según palabras de Puccinelli como "una variable o subtipo de amparo: en síntesis, un amparo especializado que, por su inserción normativa, constituye un proceso constitucional". [193] Esta particularidad es bastante inusual dentro de las normativas mundiales que reconocen esta acción.

De este artículo, en virtud de la expresión "Toda persona" también se desprende que esta acción ampara tanto a personas naturales como jurídicas.

Normas de Derecho Interno:

A nivel latinoamericano, una de las leyes que encontró mas trabas para ser promulgada es la ley 25.326 o Ley de Habeas Data del año 2000.[194] Esta ley contiene una serie de particularidades que merecen ser mencionadas.

El artículo primero habla de su objeto. Una de sus peculiaridades es que considera dentro de los sujetos activos a las "personas de existencia ideal", a las cuales se les permite actuar conjuntamente con el Defensor del Pueblo. Reza así dicho artículo:

"Artículo 1º *Objeto*. La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

---

[191] Dentro de la República Argentina, diversos de sus estados consagraron en sus constituciones internas el habeas data, pero en esta ocasión y por razones de espacio, solo me remitiré a la Constitución Federal.

[192] Artículo 43 de la Constitución Federal de la República Argentina.

[193] Oscar PUCCINELLI, El Habeas Data en Indoiberoamérica, pág. 233, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1999.

[194]Recordemos que en 1996, el Congreso de la Nación aprobó la ley 24.745, regulatoria del hábeas data, que fue vetada por decreto 1616/96 del Poder Ejecutivo y, por ende, no entró en vigor. Solo será para el año 2000 que definitivamente el habeas data se incorpore con una norma expresa al ordenamiento jurídico argentino.

Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.

En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas".[195]

Insiste así mismo esta ley en su artículo quinto que el tratamiento de datos personales es ilícito cuando no hubiere consentimiento de por medio por parte de su titular. Así miso, se debe comunicar a los titulares cuando se recaben datos sobre ellos y el fin que pretende dárseles (art. 6).

Otra de las peculiaridades de la ley argentina es que, a diferencia de otras legislaciones latinoamericanas, efectivamente regula la transmisión de datos al extranjero, por lo cual se consagra que:

> "Art. 12**.** *Transferencia internacional*.
>
> 1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados".[196]

Resulta curioso sin embargo que este cuerpo legislativo no se refiera a lo que debe entenderse por "niveles de protección adecuados", cosa que si se ha hecho por ordenamientos jurídicos como los europeos.

Esta Ley contempla un *Registro de Archivo de Datos*, el cual pretende obtener una individualización tanto del responsable como del archivo mismo. De ello trata el artículo 21.

Se establece también un *Órgano de Control*, el cual "deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley" según el artículo 29. Dicho Órgano, dispone el mismo artículo, "será dirigido y administrado por un director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia". Se trata de un órgano de control que goza de autonomía funcional y actúa como órgano descentralizado en el ámbito del Ministerio de Justicia de la Nación. De todo ello se desprende que tal *Órgano* se asemeja mucho en cuanto a sus atribuciones y objetivos con los órganos creados por las legislaciones europeas.

Otra particularidad que asemeja a la ley argentina con las europeas es la adopción de los llamados *Códigos de Conducta*, los cuales, consagrados en el artículo trigésimo disponen que:

> "Art. 30. *Códigos de conducta.*
>
> 1.- Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el

[195] Artículo primero de la Ley 25.326 de Habeas data de la República Argentina, aprobada en 2000.
[196] Artículo 12 de la Ley 25.326 de Habeas data de la República Argentina, aprobada en 2000.

tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley.

2.- Dichos códigos deberán ser inscritos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia". [197]

En cuanto al reconocimiento de la protección al derecho a la vida privada en medios de comunicación como Internet, los venezolanos Rosemberg Y Sánchez Sánz señalan que "sí existe protección para datos tales como e-mails y otros archivos almacenados en computadoras. En efecto, en abril de 1999, la Corte Penal de Apelaciones 6ta de Buenos Aires reconoció la existencia del derecho a la privacidad de los e-mails basándose en una interpretación extensiva de un artículo del Código Penal argentino que protege la privacidad de los secretos."[198] De ello se desprende que existen un reconocimiento jurisprudencial, mas no legal del tema.

[197] Artículo 30 de la Ley 25.326 de Habeas data de la República Argentina, aprobada en 2000.

[198] Alexander ROSEMBERG HOLCBLAT y Moriah SÁNCHEZ SANZ, El derecho a la privacidad en Internet, pág. 52, de texto publicado en http://vlex.com/redi/No._37_-_Agosto_del_2001/5, visitada en diciembre del año 2001.

CAPÍTULO III: LA PROTECCIÓN DEL DERECHO A LA VIDA PRIVADA EN EL ORDENAMIENTO JURÍDICO CHILENO

El derecho a la intimidad de las personas, al igual que muchos derechos de carácter constitucional, ha sufrido una serie de cambios en los sistemas jurídicos del mundo. Como consecuencia de ello, en muchos ordenamientos se ha pretendido crear normas que permitan buscar mayores garantía. Chile no ha sido la excepción, y es así que el derecho a la vida privada de las personas ha encontrado un reconocimiento más amplio tanto a nivel constitucional como a nivel de otras normas de distinto rango.

A través del presente capítulo haré un breve análisis del reconocimiento jurídico que el sistema chileno ha dado a la protección del derecho a la privacidad de las personas, partiendo de las normas constitucionales, para después continuar con los Códigos de la República, así como también respecto de ciertas normas, leyes, decretos y finalmente proyectos de ley que actualmente se encuentran en trámite en el Congreso. De ello se desprende que en los últimos diez años, la protección del derecho a la vida privada se ha visto favorecido por nuevas normas de resguardo. Sin embargo, muchas de las garantías que el ordenamiento jurídico otorga a la protección del derecho a la vida privada pueden verse amenazadas mediante el uso de Internet, en distintos ámbitos y en distintos campos, como se verá a continuación.

Códigos de la República

Constitución de 1925

La Constitución de 1925, dentro de sus garantías constitucionales no había contemplado la protección del derecho a la vida privada de una manera directa y específica. Sin embargo, el artículo décimo amparaba la inviolabilidad del hogar y de la correspondencia, que bien podrían considerarse como parte de la esfera íntima de las personas. Dicho artículo manifestaba que:

"Artículo 10.- Asimismo, la Constitución asegura a todos los habitantes de la República:

12°.- La inviolabilidad del hogar. La casa de toda persona que habite el territorio chileno sólo puede ser allanada por un motivo especial determinado por la ley, y en virtud de orden de autoridad competente;

13°.- La inviolabilidad de la correspondencia epistolar y telegráfica y de las comunicaciones telefónicas. No podrán abrirse, ni interceptarse, ni registrarse los papeles o efectos públicos, sino en los casos expresamente señalados por la ley;"[199]

[199] Artículo 10 de la Constitución de 1925, numerales 12° y 13°.

Existía sin embargo un vacío en cuanto a que no se contemplaba una protección a la vida privada de las personas propiamente tal. Aún cuando el hogar y la correspondencia forman parte de la esfera privada de los hombres, no se consideraron otros factores como proteger por ejemplo el derecho a ser dejado en paz o ampliar esta protección al círculo familiar del afectado.

Constitución de 1980

La Comisión de Estudio de la Nueva Constitución, en adelante C.E.N.C., consideró dentro de las garantías fundamentales que merecían ser protegidas por el Código Político al *derecho a la vida privada*. Ya durante su proceso de gestación, muchos miembros de la citada comisión se refirieron a la importancia de este derecho. Uno de los argumentos más brillantes, desde mi punto de vista, frente a la discusión sobre la significación humana y jurídica que el derecho a la intimidad debe tener, es el del profesor don Alejandro Silva Bascuñan, quien diría:

"Para completar la explicación de la sustancia de este precepto, desea poner de relieve su trascendencia en este momento que vive el mundo. Por un lado, el proceso de socialización ha producido una interpretación enorme entre la persona y la sociedad, y ya no puede concebirse el desarrollo de la persona humana en forma individual. Por otra parte, la sociedad influye enormemente y determina en muchos aspectos al individuo; todo lo cual hace que sea muy importante que ese proceso de penetración de la sociedad sobre el hombre tenga un límite que le permita a éste formar, consolidar y desarrollar su propia personalidad. Y es en este sentido que se le atribuye trascendencia a la aprobación de este precepto, porque frente a una sociedad que de tal manera abruma al hombre dentro de la riqueza de los medios que tiene para influir sobre él, es terriblemente dañino que la sociedad se masifique totalmente en un proceso en el cual los valores no sean puestos de relieve."[200] (subrayado es mío).

Desde esta perspectiva, merece darle importancia al alcance en el tiempo que el legislador quiso darle a este derecho, conciente respecto de los cambios que toda sociedad sufre y además conciente de los medios que el hombre dispone para amenazar derechos de carácter fundamental, como en la actualidad lo hace Internet y como se pretenderá demostrar en este trabajo.

Es así que la Constitución Política de la República ha establecido que:

"Artículo 19.- La Constitución asegura a todas las personas:

N° 4.- El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia.

[200] Enrique EVANS DE LA CUADRA, Los Derechos Constitucionales, Tomo I, Editorial Jurídica de Chile, Santiago, 1986, págs. 172 y 173.

La infracción de este precepto, cometida a través de un medio de comunicación social, y que consistiere en la imputación de un hecho o acto falso, o que cause injustificadamente daño o descrédito a una persona o a su familia, será constitutiva de delito y tendrá la sanción que determine la ley. Con todo, el medio de comunicación social podrá excepcionarse probando ante el tribunal correspondiente la verdad de la imputación, a menos que ella constituya por sí misma el delito de injuria a particulares. Además, los propietarios, editores, directores y administradores del medio de comunicación social respectivo serán solidariamente responsables de las indemnizaciones que procedan". [201]

La Carta Política chilena tiende a garantizar la vida privada desde dos puntos: su *respeto* entendiéndose por éste según el Diccionario de la Real Academia Española como "veneración, acatamiento que se hace a uno; miramiento, consideración, deferencia"[202]; y además su *protección*, definida por el mismo diccionario como "acción y efecto de proteger". Por su parte, se define al verbo *proteger* como "amparar, favorecer, defender; resguardar a una persona, animal o cosa de un perjuicio o peligro, poniéndole algo encima, rodeándole, etc".[203]

Con respecto al inciso segundo de este numeral, se hace una especial mención frente a la potencial amenaza que representan los medios de comunicación social, y en lo que respecta a este trabajo, es preciso determinar si Internet efectivamente puede o no considerarse un medio de comunicación social. En todo caso, tocaré este punto en el siguiente capítulo, al analizar las características que presenta la red.

Conforme al alcance que gran parte de la doctrina ha señalado se le debe dar al derecho a la intimidad, deben considerarse, entre otras cosas, dentro de la esfera de la vida privada de las personas el hogar, los documentos privados y las comunicaciones. Es por ello que al hacer mención de la protección constitucional que el ordenamiento jurídico chileno otorga a la vida privada de las personas, debe ser mencionado el numeral quinto del décimo noveno artículo, el cual dispone que:

"Artículo 19.- La Constitución asegura a todas las personas:

N° 5.- La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley."[204]

Resulta interesante considerar la expresión "toda forma de comunicación privada", ya que de esta manera se puede interpretar que la Constitución ampara dentro de estas nuevas formas de comunicarse a través de

[201] Artículo 19 n°4 de la Constitución Política de la República de Chile.

[202] Diccionario de la Lengua Española, Real Academia Española, Vigésima Primera Edición, Madrid, 1992, pág 1264.

[203] Ibídem, pág. 1192.

[204] Artículo 19 n°5 de la Constitución Política de la República de Chile.

Internet por ejemplo al correo electrónico. De acuerdo a este criterio, existiría una protección de rango constitucional frente a la amenaza que las nuevas tecnologías representan; sin embargo, existen todavía muchas formas de atentar contra la vida privada de las personas a través de la tecnología que todavía están impunes.

Por ello, es prudente dejar constancia que la Carta Fundamental chilena no ha contemplado la protección de la vida privada de las personas frente a la informática, tendencia ésta que se ha visto reflejada en otros textos constitucionales como los de España y de Portugal. [205]

Código Penal:

Dentro de las normas penales, la protección del derecho a la vida privada de las personas es bastante reciente. Con la Ley 19.423, promulgada con fecha 10 de noviembre de 1995 y publicada diez días más tarde, se agregaría un artículo único en el Código Penal al Título III del Libro Segundo, con el siguiente párrafo 5:

"& 5. De los delitos contra el respeto y protección a la vida privada y pública de la persona y su familia.

Artículo 161-A.- Se castigará con la pena de reclusión menor en cualquiera de sus grados y multa de 50 a 500 Unidades Tributarias Mensuales al que, en recintos particulares o lugares que no sean de libre acceso al público, sin autorización del afectado y por cualquier medio, capte, intercepte, grabe o reproduzca conversaciones o comunicaciones de carácter privado; sustraiga, fotografíe, fotocopie o reproduzca documentos o instrumentos de carácter privado; o capte, grabe, filme o fotografíe imágenes o hechos de carácter privado que se produzcan, realicen, ocurran o existan en recintos particulares o lugares que no sean de libre acceso al público.

Igual pena se aplicará a quien difunda las conversaciones, comunicaciones, documentos, instrumentos, imágenes y hechos a que se refiere el inciso anterior.

En caso de ser una misma la persona que los haya obtenido y divulgado, se aplicarán a ésta las penas de reclusión menor en su grado máximo y multa de 100 a 500 Unidades Tributarias Mensuales.

Esta disposición no es aplicable a aquellas personas que, en virtud de ley o de autorización judicial, estén o sean autorizadas para ejecutar las acciones descritas.

Artículo 161-B.- Se castigará con la pena de reclusión menor en su grado máximo y multa de 100 a 500 Unidades Tributarias Mensuales, al que pretenda obtener la entrega de dinero o bienes o la realización de cualquier conducta que no sea jurídicamente obligatoria, mediante cualquiera de los actos señalados en el

[205] El artículo 18.4 de la Constitución de España establece que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Por su parte, el Código Político de Portugal señala en el inciso segundo de su artículo 35 que "No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos".

artículo precedente. En el evento que se exija la ejecución de un acto o hecho que sea constitutivo de delito, la pena de reclusión se aplicará aumentada en un grado."[206]

De este artículo se desprende una importante enumeración que el legislador hace de las distintas maneras de atentar contra el respeto y protección de la vida privada de las personas. Nuevamente, al referirse a una invasión de la intimidad por "cualquier medio" se está dejando la puerta abierta a la utilización de medios como Internet.

Así mismo, a través de la red es perfectamente posible captar, interceptar, grabar o reproducir conversaciones o comunicaciones de carácter privado. Es también muy factible sustraer, fotocopiar o reproducir documentos o instrumentos de carácter privado, así como captar o grabar hechos de carácter privado tanto en lugares públicos como privados. Por consiguiente, de todo esto se puede desprender que Internet es un medio extremadamente poderoso, ya que, a diferencia de otros medios, éste tiene la capacidad de atentar contra la vida privada de las personas a través de un sinnúmero de vías.

Nuevo Código de Procedimiento Penal:

La Ley 19.696, promulgada el 29 de septiembre del 2000 y publicada el 12 de octubre del mismo año introdujo el nuevo Código de Procedimiento Penal. El Título III de este cuerpo legislativo establece en su párrafo segundo los "Principios de Juicio Oral". Ahí se reconoce la importancia de resguardar la vida privada del procesado, y dentro de esta política, el artículo 289 consagra que:

"Artículo 289.- Publicidad de la audiencia del juicio oral. La audiencia del juicio oral será pública, pero el tribunal podrá disponer, a petición de parte y por resolución fundada, una o más de las siguientes medidas, cuando considerare que ellas resultan necesarias para proteger la **intimidad**, el honor o la seguridad de cualquier persona que debiere tomar parte en el juicio o para evitar la divulgación de un secreto protegido por la ley :

a) Impedir el acceso u ordenar la salida de personas determinadas de la sala donde se efectuare la audiencia;

b) Impedir el acceso del público en general u ordenar su salida para la práctica de pruebas específicas, y

c) Prohibir al fiscal, a los demás intervinientes y a sus abogados que entreguen información o formulen declaraciones a los medios de comunicación social durante el desarrollo del juicio.

Los medios de comunicación social podrán fotografiar, filmar o transmitir alguna parte de la audiencia que el tribunal determinare, salvo que las partes se opusieren a ello. Si sólo alguno de los intervinientes se opusiere, el tribunal resolverá". [207] (negrilla es mía)

[206] Artículo 161-A y 161-B del Código Penal de la República de Chile.

De este artículo puede desprenderse la importancia que el legislador le ha dado a la vida privada de los procesados, velando a su vez por su honor y su seguridad e incluso por el secreto del proceso. Se trata también de una confrontación entre el principio procesal de la publicidad de la audiencia y la libertad de información, que en casos fundados, quedan desplazadas cuando el resguardo de la esfera íntima de quienes participan en un juicio oral así lo amerita. Esta norma se ajusta de esta manera a principios que, desde mi punto de vista, no pueden ser dejados de lado al momento de buscar garantizar un debido proceso .

Código del Trabajo:

La Ley 19.759, promulgada con fecha 29 de octubre de 2001 y publicada en el Diario Oficial el 10 de noviembre del mismo año es también una muestra de la intención del legislador por amparar la intimidad de las personas, en este caso particular la vida privada del trabajador en su lugar de trabajo. Así lo dispuso la mencionada Ley:

"Incorpórase en el artículo 5º, el siguiente inciso primero, nuevo, pasando los actuales incisos primero y segundo a ser incisos segundo y tercero, respectivamente:

Artículo 5º.- El ejercicio de las facultades que la ley le reconoce al empleador, tiene como límite el respeto a las garantías constitucionales de los trabajadores, en especial cuando pudieran afectar la **intimidad**, la **vida privada** o la honra de éstos."[208] (negrilla es mía).

De este inciso primero merece hacerse algunas observaciones. En cuanto al texto propiamente tal, el legislador parece hacer una distinción entre *intimidad* y *vida privada*, como si se tratara de una diferencia entre género y especie. Esto resulta curioso ya que muchas veces tanto a nivel doctrinario como legislativo e incluso jurisprudencial se ha utilizado estas dos palabras como sinónimos. Es una muestra más de que a este respecto, todavía no hay nada definitivo.

Debe dentro de todo considerarse un avance notable para quienes creemos que el derecho a la intimidad de las personas merece ser resguardado a través del perfeccionamiento y creación de normas. De hecho, en la actualidad se han dado muchos casos de amenaza al respeto de la vida privada de los trabajadores por parte del empleador, y sólo a nivel de Internet esto se ha producido a modo de ejemplo por la intercepción de la correspondencia electrónica de los trabajadores, o la utilización de la red como un medio para controlar arbitrariamente la rutina laboral de los empleados.

Código Sanitario:

---

[207] Artículo 289 del Código de Procedimiento Penal de la República de Chile.

[208] Artículo 5, inciso primero del Código del Trabajo de la República de Chile.

La Ley 19.628, también conocida como la Ley Sobre Protección de la Vida Privada, promulgada el 18 de agosto de 1999 y publicada el 28 de septiembre del mismo año, consagra en su Título Final los incisos segundo y tercero del artículo 127 del Código Sanitario. En esta modificación se pretende proteger la vida íntima de las personas a través de que los servicio relacionados con la salud sean reservados y no tengan el carácter de públicos. Así lo expresan los mencionados incisos:

"Artículo 127.- Incisos segundo y tercero:

Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo.

Lo dispuesto en este artículo no obsta para que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos".[209]

Decretos de la República

Decreto 643 sobre el Reglamento de visitas de abogados y demás personas habilitadas en los establecimientos penitenciarios:

Siguiendo con la tendencia a proteger la vida privada de los procesados es que procedo a mencionar este decreto, promulgado con fecha 17 de julio del 2000 y publicado en el Diario Oficial el 25 de octubre del mismo año. Es así que el artículo noveno del Título III establece que:

"Artículo 9.- En todos los establecimientos penitenciarios se habilitarán dependencias que reúnan condiciones de **privacidad** y comodidad indispensables para la atención profesional de los internos, para cuyo efecto el personal de vigilancia prestará la necesaria colaboración.

En los establecimientos o secciones especiales de alta seguridad, en donde además de las salas para visitas de abogados, existan locutorios para que los reclusos conferencien con los abogados o demás personas habilitadas, debido a su alto compromiso delictual y peligrosidad, se estará a la normativa interna

[209] Artículo 127, incisos segundo y tercero del Código Sanitario de la República de Chile.

del establecimiento para determinar el lugar en donde se realizará la atención profesional".[210] (negrilla es mía).

Decreto 553 sobre el Reglamento aplicable a menores de edad internos en establecimientos administrados por gendarmería de Chile:

El ordenamiento jurídico chileno ha sido cuidadoso en resguardar el derecho a la intimidad de los menores de edad, conciente de que ello es necesario para un adecuado desarrollo personal. Desde esta perspectiva, esta norma promulgada el 7 de junio del año 2001 y publicada en el Diario Oficial el 22 de enero del 2002 consagra en su artículo sexto dentro de las Disposiciones Preliminares lo siguiente:

"Artículo 6º: Se garantiza la libertad ideológica y religiosa de los menores internos, su derecho al honor, a ser designados por su propio nombre, a la **intimidad** personal, a la información, a la educación y el acceso a la cultura, procurando el desarrollo integral de su personalidad, y a elevar peticiones a las autoridades, en las condiciones legalmente establecidas".[211] (negrilla es mía).

De lo anteriormente expuesto resulta interesante detenerse en la expresión *intimidad personal*, partiendo de la base que algo "personal" es algo propio o particular de la persona, por lo cual, parece curioso que el legislador haya hecho esta especificación de la intimidad cuando ella por sí misma representa una parte propia o particular de la vida de las personas. Sin embargo, analizando más el fondo y no la forma, es importante este reconocimiento, el cual insiste en una serie de garantías constitucionales que pretenden proteger también la vida íntima de los menores desde su corta edad.

Decreto 730 sobre el Reglamento para la aplicación del Título IV de la Ley 16.618 sobre casas de menores e instituciones asistenciales:

Esta norma fue promulgada el 19 de julio de 1996 y publicada en el Diario Oficial el 3 de diciembre del mismo año, y refiriéndose a la estructura de estos centros dispone que:

"Artículo 21°.- Cada Centro deberá contener en el Reglamento Interno normas en que se establecerá:

1.- Número de casas o pabellones y dependencias con que cuenta el Centro.

2.- El fin a que estará destinada cada casa o dependencia.

3.- Las características de los niños y jóvenes de acuerdo a las cuales se determinará su ingreso a las casas o pabellones.

[210] Artículo 9 del Decreto 643 sobre las visitas de abogados y demás personas habilitadas en los establecimientos penitenciarios, de la República de Chile.

[211] Artículo 6 del Decreto 553 sobre el Reglamento aplicable a menores de edad internos en establecimientos administrados por gendarmería de Chile.

4.- La cantidad máxima de niños y jóvenes que puede albergar cada casa o pabellón la que se determinará teniendo en cuenta factores tales como su dignidad, su necesidad de **intimidad**, la seguridad, la higiene.

5.- El número de aposentos destinados a dormitorios y su capacidad".[212] (negrilla es mía).

Siguiendo una política destinada a la protección de la intimidad de los menores, este decreto también vela por un ambiente adecuado para que los menores desarrollen su "necesidad de intimidad".

Decreto 570 que aprueba el reglamento para la intervención de las personas con enfermedades mentales y sobre los establecimientos que las proporcionen:

Este Decreto fue promulgado el 28 de agosto de 1998 y publicado en el Diario Oficial con fecha 14 de julio del año 2000, y consagra que:

"Artículo 35.- Todo paciente tendrá derecho a que se resguarde su seguridad personal y la confidencialidad de su estadía y tratamiento dentro del establecimiento, a mantener el ejercicio de su **vida privada** en cuanto sea compatible con éste y a no ser sometido a investigaciones y estudios no autorizados por él".[213] (negrillas son mías).

El legislador ha querido resguardar la confidencialidad de la estadía de quienes pasan o han pasado por estos establecimientos para enfermos mentales. Es una muestra clara por proteger aquellos aspectos de la vida de las personas que no se quiere que sean divulgados a terceros. Resulta también prudente detenerse en la expresión "mantener el ejercicio de su vida privada", ya que se está reconociendo de esta manera cuan importante se vuelve *ejercitar* aquella esfera propia de los individuos, aún cuando estos se encuentran, por modo de ejemplo, internados en centros de salud.

Decreto 2.542 aprueba el reglamento sobre reconocimiento de entidades calificadoras de incapacidad:

Con el objeto de garantizar la vida privada de los pacientes, este decreto, promulgado con fecha 15 de diciembre de 1995 y publicada en el Diario Oficial el 23 de enero del año siguiente, consagra que:

"Artículo 3°.- Las entidades que presten los servicios señalados en el artículo 1° de este reglamento, deberán cumplir las siguientes condiciones:

[212] Artículo 21 del Decreto 730 que establece el Reglamento para la aplicación del Título IV de la Ley 16.618 sobre casas de menores e instituciones asistenciales de la República de Chile.
[213] Artículo 35 inciso tercero del Decreto 570 que aprueba el reglamento para la intervención de las personas con enfermedades mentales y sobre los establecimientos que las proporcionen, de la República de Chile.

a) Disponer de un local exento de barreras arquitectónicas y dotado con las comodidades mínimas necesarias para efectuar la atención de los pacientes y los exámenes y reconocimientos correspondientes, en condiciones técnicas y de **privacidad** adecuadas".[214] (negrilla es mía).

Decreto 466 que imparte normas para la aplicación de un programa de vigilancia epidemiológica del Sida:

Esta norma tiene especial importancia en cuanto se ha tomado conciencia de proteger la vida de quienes están especialmente discriminados, como es el caso de los enfermos de SIDA. Así, esta Ley promulgada el 12 de junio de 1987 y publicada el 14 de noviembre del mismo año establece que:

"Artículo 7°.- El Ministerio de Salud velará especialmente para que se cautele y haga efectivo el derecho a la **privacidad** de los enfermos de SIDA, de los portadores de serología positiva, de los contactos y los respectivos grupos familiares". [215] (negrilla es mía).

Decreto 26 que aprueba el Reglamento sobre el secreto o reserva de los actos y documentos de la administración del Estado:

Fue promulgado con fecha 28 de enero del 2001 y publicado en el Diario Oficial el 7 de mayo del mismo año 2001. Dentro de sus normas, merece ser nombrada para efectos de este trabajo, la siguiente:

"Artículo 8º.- Sólo podrán ser declarados como secretos o reservados los actos y documentos cuyo conocimiento o difusión pueda afectar el interés público o privado de los administrados, de conformidad a los criterios que se señalan a continuación.

b) La declaración de secreto o reserva basada en la protección de intereses privados de los administrados, procederá respecto de los siguientes actos y documentos:

2. Aquellos cuya comunicación o conocimiento afecte la **vida privada** de una persona individualizada o identificable".[216] (negrillas son mías).

---

[214] Artículo 3, literal a) del Decreto 2542 que aprueba el reglamento sobre reconocimiento de entidades calificadoras de discapacidad, de la República de Chile. Dentro de esta misma tendencia, el Decreto 2298, promulgado el 10 de octubre de 1995 y publicado el 5 de febrero de 1996, en su artículo 16 señala que "Todos los pacientes que se encuentren en régimen de internación tendrán derecho a la recreación y a contar con espacios para ello. Así mismo, deberán contar con un espacio que les permita privacidad si así lo requieren, de acuerdo a las condiciones del programa de rehabilitación".

[215] Artículo 7 del Decreto 466 que imparte normas para la aplicación de un programa de vigilancia epidemiológica del Sida. Siguiendo esta misma tendencia, el Decreto 712, promulgado el 8 de noviembre de 1999 y publicado el 17 de abril del 2000, que aprueba Reglamento sobre notificación de enfermedades transmisibles de declaración obligatoria.

[216] Artículo 8, punto 2 del literal b) del Decreto 26 que aprueba el Reglamento sobre el secreto o reserva de los actos y documentos de la administración del Estado de Chile.

Decreto 220 que aprueba el Reglamento de Homologación de Aparatos Telefónicos:

Este decreto, promulgado con fecha 5 de diciembre de 1980 y publicado el 8 de enero de 1981, dentro del título "Equipos multilíneas y secretariales" consagra el derecho a la privacidad dentro de las comunicaciones, por lo cual se establece que:

"Artículo 18.- Detalle de las especificaciones.

d) En el caso de corte de la energía eléctrica que alimenta la unidad básica, el sistema debe poder seguir recibiendo llamadas desde la red telefónica siendo anunciadas, en este caso, con señalización audible.

Debe existir secreto total (**privacidad**) en las comunicaciones y la posibilidad de anular dicha condición, si los requerimientos del usuario así lo determinan". (negrilla es mía).

Se trata de una muestra más en que se consagra el secreto de las comunicaciones, y como veremos más adelante, Internet es un medio de comunicación que puede utilizarse a través de las líneas telefónicas, por consiguiente, su resguardo también se encontraría garantizado.

Decreto 321 que crea la Comisión Nacional para las nuevas tecnologías de información y de comunicación:

Este decreto, promulgado el 18 de junio de 1998 y publicado dos meses más tarde establece en su sexto considerando que:

"Considerando 6.- La conveniencia de contar con una propuesta respecto de los fundamentos sobre la base de los cuales sea posible abordar, con criterios regulatorios, materias tales como la **privacidad** de las comunicaciones, la seguridad de los datos, la compatibilización de normas estándares, la garantía de acceso, la libre expresión y la protección contra abusos".[217] (negrilla es mía).

Se trata de prevenir nuevas maneras de atentar, entre otras cosas, contra el derecho a la vida privada de las personas a través de nuevas tecnologías de información y de comunicación. Dentro de ellas encaja perfectamente Internet, que se vuelve también una amenaza contra garantías como las que este considerando menciona. Lamentablemente, en la práctica poco se conoce de esta Comisión Nacional y su aporte al resguardo de la intimidad de las personas no se ha reflejado mucho en la práctica.

Leyes de la República

Ley de Tránsito:

[217] Considerando sexto del Decreto 321 que crea la Comisión Nacional para las nuevas tecnologías de información y de comunicación, de la República de Chile.

El 28 de abril del año 2000 fue promulgada la Ley 19.676, que modifica la Ley 18.287 sobre procedimiento ante los juzgados de policía local y la Ley 18.290 de Tránsito. Esta Ley fue publicada a su vez en el Diario Oficial con fecha 29 de mayo del 2000. Tiene por objeto regular el uso de los equipos de registro de que disponen tanto carabineros como inspectores fiscales o municipales. Es así que la ya citada ley dispone que:

"Artículo 2º.- Introdúcese las siguientes modificaciones en la ley Nº18.290 de Tránsito.

1. Agréganse los siguientes incisos al artículo 4º:

Para los efectos del inciso anterior, los mencionados funcionarios podrán operar directamente, sea en forma próxima o a distancia, equipos de registro de infracciones que se ajusten a lo dispuesto en los incisos siguientes.

Los equipos de registro de infracciones podrán consistir en películas cinematográficas, fotográficas, fonográficas u otras formas de reproducción de la imagen y del sonido y, en general, en medios aptos para producir fe.

Las normas de tránsito cuyo cumplimiento se fiscalice mediante el uso de los equipos antes mencionados deberán estar señalizadas de conformidad a las disposiciones del Manual de Señalización de Tránsito, cuando corresponda.

El reglamento, que se expedirá por intermedio del Ministerio de Transportes y Telecomunicaciones contemplará los estándares técnicos que tales equipos deberán cumplir en resguardo de su confiabilidad y certeza, y establecerá las condiciones en que han de ser usados para que las imágenes u otros elementos de prueba que de ellos se obtengan puedan servir de base para denunciar infracciones o contravenciones. Entre estas últimas, dispondrá especialmente la existencia de señales de tránsito que adviertan con claridad y en forma oportuna a los conductores los sectores en que se usan estos equipos; y adoptará medidas tendientes a asegurar el respeto y protección a la vida privada, tal como la prohibición de que las imágenes permitan individualizar a los ocupantes del vehículo. (...)".[218] (subrayado es mío).

Entre los equipos de registro de infracciones que contempla la ley se encuentran "otras formas de la reproducción de la imagen y del sonido". Dentro de estas *otras formas* podría utilizarse Internet, ya que es una vía fácil y efectiva para reproducir tanto imágenes como sonidos. Claro que, como acertadamente lo establece la propia Ley, el uso de estos equipos encuentra un límite en el respeto y protección de la vida privada de los ciudadanos.

El ejemplo que esta norma otorga se refiere a la prohibición de que se individualice a los ocupantes de un vehículo. Se trata de apenas un caso común, que entre tantos otros, es utilizado por entes de carácter público y que representa un atentado a la esfera íntima de las personas.

[218] Artículo 4 de la Ley de Tránsito n° 18.290 de la República de Chile.

Ley 19.733 sobre libertades de opinión e información y ejercicio del periodismo:

Esta Ley fue publicada en el Diario Oficial con fecha lunes 4 de junio del año 2001. Con ella se pretendió regular los derechos de los medios de comunicación social, especialmente en cuanto a su libertad de opinión e información. Existe sin embargo dentro de la doctrina un debate sobre si Internet forma parte o no de estos medios (como se señalaba ya cuando se trató el art. 19N°4, inciso segundo de la Constitución), y por consiguiente si esta ley se aplica o no a la red de redes. Sin embargo, nadie niega que, dentro de quienes hacen uso de la red, se encuentran medios de comunicación tradicionales, como los medios escritos, la radio o la televisión, que tienen en muchos casos un espacio virtual.

Dentro de las normas que consagra el párrafo tercero de esta Ley, relativa a los delitos cometidos a través de un medio de comunicación social, es prudente mencionar al artículo 29 en el cual se reconocen y castigan los delitos de injuria y calumnia, y además citar el inciso final del artículo 30 que dice:

"Artículo 30.- Inciso Final:

Se considerarán como pertenecientes a la esfera privada de las personas los hechos relativos a su vida sexual, conyugal, familiar o doméstica, salvo que ellos fueren constitutivos de delito".[219] (subrayado es mío).

Muchas veces, abusando en el ejercicio de los derechos de libertad de expresión e información se ha atentado contra la vida privada de las personas. Es por ello que esta norma ha pretendido dar a conocer hechos considerados como pertenecientes a la esfera íntima de las personas, para de esta manera dejar establecido que los derechos de los medios de comunicación social no son absolutos y tienen dentro de sus límites el respeto a la vida íntima de las personas. La enumeración que este artículo hace de los hechos pertenecientes a la esfera privada de las personas no puede, en todo caso, considerarse como taxativa.

Ley 19.628 sobre Protección de la Vida Privada:

Esta Ley, que representa un paso importante en cuanto a al protección de la vida privada de las personas dentro del ordenamiento jurídico chileno (aun cuando de ella puedan surgir algunas críticas), encontró dentro de sus fuentes a la Ley Orgánica número 1, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen y a la LORTAD en España[220]; a la ley francesa de informática, ficheros y libertades de 1978; las leyes de protección de datos de Noruega de 1978 y de Gran Bretaña de 1984; en

[219] Artículo 30 de Ley 19.733 sobre libertades de opinión e información y ejer4cicio del periodismo.

[220] Se la conoce como la ley orgánica número 1, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Por su parte, las siglas de la LORTAD responden a la "Ley Orgánica de Regulación de Tratamiento Automatizado de Datos", de 1992.

Alemania lo que el Tribunal Constitucional germano ha reconocido como el derecho a la autodeterminación informativa, entre otros textos.

Nació a raíz del proyecto de ley que presentara el senador Canturias en la sala del Senado el 5 de enero de 1993. [221] El texto sería aprobado por el Senado con fecha 4 de octubre de 1995.

Haciendo un breve análisis de lo que fue le proceso de gestación y desarrollo de esta Ley, Christian Suárez Crothers señala que "se concibe a la vida privada como comprensiva de a lo menos cuatro bienes jurídicos a los que se estima dignos de protección: a) el derecho a la propia imagen, b) el derecho a una vida tranquila, sin hostigamientos ni perturbaciones, c) el derecho al anonimato y la reserva y d) el derecho a la inviolabilidad del hogar de toda forma de comunicación privada". Refiriéndose a las modificaciones realizadas en la Cámara de Diputado a este proyectos, en la sesión tercera celebrada en junio de 1996, el propio Suárez Crothers indica que: "En cuanto a los aspectos de fondo, llama la atención que el proyecto parta de la base de reconocer a toda persona el derecho a recolectar, procesar, custodiar y transferir datos (art.1°), cuando lo que las técnicas de protección de datos tratan de lograr no es ampliar las posibilidades jurídicas de los individuos para recoger informaciones de los demás, sino precisamente todo lo contrario. Porque, si se quiere comprender bien el fenómeno que debe ser objeto de la regulación, se debe partir del reconocimiento del derecho a la libertad informática de los individuos y no del derecho general a recolectar y difundir información, porque este último, si hemos de concebirlo como un derecho, está llamado a ocupar un lugar distinto del que es ahora objeto de preocupación por los legisladores". [222]

Finalmente, el 18 de agosto de 1999 sería promulgada la Ley 19.628 Sobre Protección de la Vida Privada, y publicada en el Diario Oficial diez días más tarde.

Sin pretender hacer un estudio minucioso y profundo de esta ley, al alejarse esto del objetivo de este trabajo, procederé a hacer un breve análisis de sus principales puntos.

Objeto: La presente Ley tiene por objeto el asegurar a las personas el respeto a su intimidad en lo referente al tratamiento de datos de carácter personal en registros o bancos de datos por organismos públicos o particulares. Así lo dispone el artículo primero que señala que:

"Artículo 1°.- El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se

[221] El objetivo de este proyecto de ley, según los estudios de Puccinelli, pretendía crear un "Código o estatuto jurídico de la privacidad, brindar una adecuada protección a la privacidad de las personas en el ámbito del derecho civil (donde se evidencia un vacío legislativo), y concentrar otras disposiciones incorporadas en el proyecto de ley sobre las libertades de opinión e información y el ejercicio del periodismo".

[222] Citado por Oscar Puccinelli en El Habeas Data en Indoiberoamérica, pág. 342, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1999.

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.

Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce."[223]

Del inciso segundo también se desprende la intención del legislador por facultar a las personas, tanto naturales como jurídicas, para manejar datos de carácter personal, estableciéndose como límites los que establece esta ley, las finalidades del ordenamiento jurídico, el pleno ejercicio de los derechos fundamentales.

Definiciones: El artículo segundo de esta ley se preocupó de definir una serie de conceptos relativos a la transferencia de datos de carácter personal. Es así que:

"Artículo 2°.- Para los efectos de esta ley se entenderá por:

a) Almacenamiento de datos, la conservación o custodia de datos en un registro o banco de datos.

b) Bloqueo de datos, la suspensión temporal de cualquier operación de tratamiento de los datos almacenados.

c) Comunicación o transmisión de datos, dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.

d) Dato caduco, el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.

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

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

g) Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

[223] Artículo primero de la Ley 19.628 sobre Protección de la Vida Privada.

h) Eliminación o cancelación de datos, la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.

i) Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.

j) Modificación de datos, todo cambio en el contenido de los datos almacenados en registros o bancos de datos.

k) Organismos públicos, las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1° de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

l) Procedimiento de disociación de datos, todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable.

m) Registro o banco de datos, el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.

n) Responsable del registro o banco de datos, la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal.

ñ) Titular de los datos, la persona natural a la que se refieren los datos de carácter personal.

o) Tratamiento de datos, cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma".[224]

En lo que respecta al tema de estudio de este trabajo, merecen especial atención las definiciones de "datos de carácter personal" y "datos sensibles". En cuanto a la primera definición, se habla de "cualquier información", lo cual es bastante amplio y puede perfectamente contener datos que no necesariamente pertenecen a aquella parte de la vida íntima de las personas. Es precisamente la definición de "datos sensibles" la que abarca información que a su vez formen parte de las "características físicas o morales de las personas" y de su "vida privada o intimidad". De ello se desprende positivamente de que se trata de datos que pertenecen a aquella esfera de la vida de las personas, calificada como personal e inaccesible frente a

[224] Artículo 2 de la Ley 19.628 sobre la Protección de la Vida Privada.

terceros. Estos datos, por regla general, no pueden transferirse[225]. Sin embargo, bajo ningún punto de vista pueden considerarse como una enumeración de carácter taxativo la lista de datos que esta definición establece.

Resulta también interesante analizar la definición de "comunicación o transmisión de datos", consagrada en el literal c) del segundo artículo de la ley. Según esta definición, comprende el "dar a conocer de cualquier forma los datos de carácter personal", y dentro de estas diversas formas puede encajar perfectamente el hacerlo a través de Internet. Por consiguiente, la utilización de este medio de comunicación se verá regulada dentro de esta norma en lo que a transferencia de datos de carácter personal se refiere.

Sujeto activo: El artículo primero de esta ley pretende regular la "protección de las personas", sin hacer una distinción entre personas naturales o jurídicas. Sin embargo, será el artículo segundo el que se encargue de precisar que los datos de carácter personal y los datos sensibles pertenecen, para efectos de esta ley exclusivamente a personas naturales. Incluso, respecto de las definiciones del artículo segundo, en el literal ñ) se establece que son "titulares de los datos" las personas naturales. Dentro de la doctrina Chilena, tanto Cifuentes Muñoz como Pfeffer son partidarios que a este respecto ha existido un error por parte del legislador al no amparar dentro de esta ley a las personas jurídicas. Aún cuando este error se ha visto bastante en la legislación latinoamericana, en lo personal creo que efectivamente debe ampliarse el ámbito de resguardo a los datos de las personas jurídicas, dentro de las cuales el problema es latente y absolutamente vigente ya que, al igual que las personas naturales, disponen de una gran cantidad de datos que han sido víctimas de un tratamiento abusivo y contrario a los principios que esta ley consagra.

Sujeto pasivo: Ya el primer artículo de esta ley parece aclarar de que sus normas se aplican tanto a "registros o bancos de datos por organismos públicos o por particulares", de lo cual se puede llegar a una aproximación de que son sujetos pasivos tanto las personas naturales como jurídicas. Incluso, este mismo artículo habla de "personas", sin hacer distinción alguna. El artículo segundo por su parte considera que son responsables del registro o banco de datos las "personas naturales o jurídicas privadas o el respectivo organismo público". Sin embargo, el artículo cuarto es más preciso en cuanto al ámbito de aplicación de esta ley, por lo cual se consagra que:

"Artículo 4.- El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.

La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.

La autorización debe constar por escrito.

[225] El artículo 10 de la Ley 19.628 establece que: "No pueden ser objeto de tratamiento de datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares".

La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito.

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

Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos".[226]

Bienes jurídicos tutelados: Esta ley tiene por objeto proteger la vida privada de las personas, así lo consagra el nombre de esta norma, y dentro de la vida privada, aquella parte que la conforman los datos de carácter personal. De ello puede a su vez desprenderse que se pretende proteger el honor y la propia imagen del ser humano. Resulta sin embargo interesante dejar constancia que esta Ley no incorpora a los conceptos de "autodeterminación informativa" o "libertad informática" y menos "habeas data", aún cuando se pretende justamente reconocer y regular este último concepto.

Del artículo quinto de esta ley se puede deducir la intención del legislador por regular la transmisión de datos a través de una "red electrónica", que si bien no es definida por la propia ley, se podría interpretar que se refiere por ejemplo a la transmisión de datos de carácter nominativo a través de Internet. Dicho artículo tiene el siguiente texto:

"Artículo 5.- El responsable del registro o banco de datos personales podrá 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 datos que se transmiten.

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.

[226] Artículo 4 de la Ley 19.628 sobre la Protección de la Vida Privada.

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

No se aplicará este artículo cuando se trate de datos personales accesibles al público en general.

Esta disposición tampoco es aplicable cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes".[227] (subrayado es mío).

Aún cuando el legislador pretendió dar la pauta de la trasmisión de datos a través de las redes electrónicas, por medio de requisitos como la individualización del requirente, la manifestación y el propósito del requerimiento o el tipo de datos que se transmiten, no tienen en la vida cuotidiana mucha relevancia en el sentido de que se vuelve difícil, por no decir imposible, velar por el respeto de tales requisitos.

El ordenamiento jurídico chileno tampoco se ha manifestado respecto de la transferencia de datos a otros países, ni tampoco respecto de las pautas de posibles códigos de conducta. Así mismo, se debe mencionar que tampoco existe una "Autoridad" que se dedique al resguardo y fiscalización del tratamiento de datos personales. De ello se desprende que la norma se torna incompleta, y que la teoría se ve opacada por como se lleva a cabo la práctica.

Ley 19.223 relativa a Delitos Informáticos:

Esta proyecto de ley se compone de cuatro artículos que son:

"Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2º.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3º.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4º.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado". [228]

[227] Artículo 4 de la Ley 19.628 sobre la Protección de la Vida Privada.

Resulta curioso que ni el ordenamiento jurídico ni esta ley definan lo que son los "sistemas de tratamiento de información" o "sistemas de información". En todo caso, podríamos remitirnos a la definición que la Ley 19.628 otorga en su artículo segundo literal o) respecto de los *tratamientos de datos* entendiéndose a estos como " cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma".

Debemos partir de la base que a través de Internet se puede perfectamente ejecutar todas las funciones que la citada definición describe. Además, no es de sorprenderse que a través de la red también es posible destruir o inutilizar un sistema de tratamiento de información; apoderarse, alterar, dañar o destruir los datos contenidos en dicho sistema, e incluso revelarlos y difundirlos. Por consiguiente, los delitos informáticos que este proyecto pretende regular pueden cometerse perfectamente a través de Internet. Del mismo modo, a través de estos ilícitos penales cometidos haciendo uso de la red, se pueden violar garantías constitucionales como el derecho a la vida privada de las personas.

Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma:

Esta Ley responde a las necesidades de un Estado de estar a la par con el desarrollo de las nuevas tecnologías. Es así que el Congreso Nacional, con fecha 14 de marzo de 2002 promulgó esta Ley, y la publicó en el Diario Oficial el 12 de abril del mismo año. Dentro del texto de esta ley, merecen ser mencionados los siguientes artículos:

" TITULO I
Disposiciones Generales

Artículo 1º.- La presente ley regula los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso.

Las actividades reguladas por esta ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte de papel.

Toda interpretación de los preceptos de esta ley deberá guardar armonía con los principios señalados.

Artículo 2º.- Para los efectos de esta ley se entenderá por:

a) Electrónico: característica de la tecnología que tiene capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;

[228] Ley 19.223 sobre Delitos Informáticos.

b) Certificado de firma electrónica: certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica;

c) Certificador o Prestador de Servicios de Certificación: entidad prestadora de servicios de certificación de firmas electrónicas;

d) Documento electrónico: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior;

e) Entidad Acreditadora: la Subsecretaría de Economía, Fomento y Reconstrucción;

f) Firma electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor;

g) Firma electrónica avanzada: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría, y

h) Usuario o titular: persona que utiliza bajo su exclusivo control un certificado de firma electrónica.(...)

TITULO III

De los Prestadores de Servicios de Certificación

Artículo 11.- Son prestadores de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar.

Asimismo, son prestadores acreditados de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, domiciliadas en Chile y acreditadas en conformidad al Título V de esta ley, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar.

Artículo 12.- Son obligaciones del prestador de servicios de certificación de firma electrónica:

b) Mantener un registro de acceso público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto, en los términos señalados en el reglamento. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto, y no podrá utilizarlos para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la ley Nº 19.628, sobre Protección de la Vida Privada;

j) Cumplir con las demás obligaciones legales, especialmente las establecidas en esta ley, su reglamento, y las leyes Nº 19.496, sobre Protección de los Derechos de los Consumidores, y Nº 19.628, sobre Protección de la Vida Privada.

Artículo 13.- El cumplimiento por parte de los prestadores no acreditados de servicios de certificación de firma electrónica, de las obligaciones señaladas en las letras a), b), c) y j) del artículo anterior, será considerado por el juez como un antecedente para determinar si existió la debida diligencia, para los efectos previstos en el inciso primero del artículo siguiente.

Artículo 14.- Los prestadores de servicios de certificación serán responsables de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas electrónicas. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.

Sin perjuicio de lo dispuesto en el inciso anterior, los prestadores no serán responsables de los daños que tengan su origen en el uso indebido o fraudulento de un certificado de firma electrónica.

Para los efectos de este artículo, los prestadores acreditados de servicios de certificación de firma electrónica deberán contratar y mantener un seguro, que cubra su eventual responsabilidad civil, por un monto equivalente a cinco mil unidades de fomento, como mínimo, tanto por los certificados propios como por aquellos homologados en virtud de lo dispuesto en el inciso final del artículo 15.

TITULO IV

De los Certificados de Firma Electrónica

Artículo 15.- Los certificados de firma electrónica, deberán contener, al menos, las siguientes menciones:

a) Un código de identificación único del certificado;

b) Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada;

c) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y su rol único tributario, y

d) Su plazo de vigencia.

Los certificados de firma electrónica avanzada podrán ser emitidos por entidades no establecidas en Chile y serán equivalentes a los otorgados por prestadores establecidos en el país, cuando fueren homologados por estos últimos, bajo su responsabilidad, y cumpliendo los requisitos fijados en esta ley y su reglamento, o en virtud de convenio internacional ratificado por Chile y que se encuentre vigente.

El certificado de firma electrónica provisto por una entidad certificadora podrá establecer límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles por tercero. El proveedor de servicios de certificación quedará eximido de responsabilidad por los daños y perjuicios causados por el uso que exceda de los límites indicados en el certificado.

En ningún caso la responsabilidad que pueda emanar de una certificación efectuada por un prestador privado acreditado comprometerá la responsabilidad pecuniaria del Estado.

TITULO VI

Derechos y Obligaciones de los Usuarios de Firmas Electrónicas

Artículo 23.- Los usuarios o titulares de firmas electrónicas tendrán los siguientes derechos:

1º. A ser informado por el prestador de servicios de certificación, de las características generales de los procedimientos de creación y de verificación de firma electrónica, así como de las reglas sobre prácticas de certificación y las demás que éstos se comprometan a seguir en la prestación del servicio, previamente a que se empiece a efectuar;

2°. A la confidencialidad en la información proporcionada a los prestadores de servicios de certificación. Para ello, éstos deberán emplear los elementos técnicos disponibles para brindar seguridad y privacidad a la información aportada, y los usuarios tendrán derecho a que se les informe, previamente al inicio de la prestación del servicio, de las características generales de dichos elemento;

Los usuarios gozarán de estos derechos, sin perjuicio de aquellos que deriven de la ley N° 19.628, sobre Protección de la Vida Privada y de la ley N° 19.496, sobre Protección a los Derechos de los Consumidores y podrán, con la salvedad de lo señalado en el número 10° de este artículo, ejercerlos conforme al procedimiento establecido en esa última normativa.

Artículo 24.- Los usuarios de los certificados de firma electrónica quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones exactas y comp letas. Además, estarán obligados a custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador, y a actualizar sus datos en la medida que éstos vayan cambiando." [229] (subrayado es mío)

Esta ley sin lugar a dudas que guarda una estrecha relación con el tema de estudio de este trabajo. Se trata desde mi punto de vista de un importante adelanto en el ordenamiento jurídico chileno. Sin embargo, creo prudente hacer unos pocos comentarios.

Cuando la ley define *electrónico*, se refiere a "toda característica de la tecnología que tiene capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares". Este concepto está muy vinculado con las nuevas tecnologías, y desde esta perspectiva debe considerarse a Internet como un medio de comunicación electrónico, y por consiguiente una alternativa de transporte de cualquier documento electrónico.

Ha sido un acierto del legislador el haber establecido dentro de las obligaciones del prestador de servicios de certificación de firma electrónica el deber de cumplir con lo que otras normas como la 19.628 establece a

[229] Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.

favor de la protección de la vida privada de las personas. Es también interesante el valor probatorio que la ley le ha otorgado a este documento.

En cuanto al certificado propiamente tal, de su naturaleza se deduce que es un dato sensible, y que además dentro de su contenido guarda datos considerados de carácter personal. Así, si bien se trata de una de las soluciones que parte de la doctrina ha propuesto para afrontar las amenazas frente a la invasión de la vida privada en sistemas como Internet, este sistema criptográfico, mal llevado, podría traer consecuencias no deseadas. Es también por ello que el legislador se ha preocupado especialmente en delimitar con el mayor detalle posible los derechos y obligaciones de aquellos que intervienen en este proceso.

Soy optimista de que en la práctica este sistema revele resultados positivos, pero no puedo dejar de manifestar mi preocupación acerca de sistemas que en un futuro, con todos los adelantos de la ciencia, comiencen a descifrar sistemas criptográficos que aparentemente se muestran en el presente como indescifrables.

Proyectos de Ley

Aparte de las normas recién descritas, existen actualmente en tramitación en el Congreso normas que tienen por objeto proteger el derecho a la intimidad de las personas, sobre todo en cuanto al peligro que representan las nuevas tecnologías y los nuevos medios de comunicación como Internet. Analicemos las siguientes propuestas del legislador:

1.- Proyecto de Ley para la Regulación de Internet.

Este proyecto fue presentado con fecha martes 7 de septiembre de 1999, en sesión ordinaria 37° [230] y dispone lo siguiente:

[230] Fue presentado por los diputados señores Velasco, Villouta, Krauss, Jarpa, Núñez, Patricio Cornejo, Vilches, Olivares, Ceroni y Reyes en boletín N° 2395-19. Allí se pronunció el siguiente discurso "Parece incontestable que una sociedad moderna y democrática no puede existir sin un sistema de medios de comunicación de masa, pero estos medios han de estar puestos a disposición del gran público y ser de fácil acceso, debiendo reflejar la naturaleza pluralista de la sociedad a la que sirven y no estar controlados, en régimen de monopolio, por ningún grupo de interés ni estar dominado por ideologías de uno u otro signo. Ello, para que puedan suministrar con imparcialidad la información necesaria para que los ciudadanos se formen una opinión clara respecto de su entorno, con conocimiento de causa. Además, para que exista un Estado democrático y una verdadera sociedad democrática con grados importantes de desarrollo y con permanencia en el tiempo, debe existir una opinión pública libre y debidamente informada. Sólo en estas condiciones es posible realizar la plena democracia política. Por ello la libertad de comunicación está en la esencia de toda estructura democrática y el derecho a la libre comunicación interpretado como derecho de prensa, información y libertad de opinión tiene un reconocimiento internacional como derecho humano. Entonces, la libertad de expresión tiene aspectos de derecho subjetivo, inherente a todas las personas por el mero hecho de ser reconocidas. Iguales en derechos a los demás, y también de derecho objetivo, como garantía institucional de un régimen democrático. No obstante, en un Estado de derecho los medios de comunicación masiva deben observar deberes y responsabilidades específicas para quienes se desempeñan en estos organismos. Esta situación que es más obvia tratándose de los medios tradicionales, es decir prensa escrita, radio y televisión, se alteran cuando se trata de defender los derechos en medios electrónicos como la Internet. En todo caso, el

"Artículo Primero.- El que difunda o propale a través de sistemas, redes y procedimientos de Internet, o de otro servicio de igual naturaleza, informaciones, contenidos o noticias contrarias a la moral, el orden público, o las buenas costumbres será sancionado con una multa de 15 Unidades Tributarias Mensuales.

Igual sanción se aplicará a quienes usen dolosamente tales servicios y redes con el propósito de incitar al odio y a la discriminación contra grupo de personas en razón de su raza, nacionalidad, sexo o religión; y a las que utilicen estos servicios o redes para difundir pornografía o efectuar una apología de violencia.

Artículo segundo.- Será competente para conocer y fallar las causas a que diere lugar la aplicación de la norma anterior, el juez de policía local correspondiente, el que aplicará el procedimiento a que se someten las causas bajo su jurisdicción.

Artículo tercero.- La autoridad respectiva tratará que en los programas de estudio de la enseñanza básica y media se contengan cursos destinados a enseñar la forma de utilizar las redes y servicios de Internet o de otros servicios de igual naturaleza, con la finalidad de difundir la cultura.

Artículo cuarto.- El que para difundir sus servicios o programas a través de las redes de Internet, utilice procedimientos que engañen sobre el contenido verdadero de los programas o servicios, será sancionado con la pena establecida en el artículo primero.

Artículo quinto.- La correspondiente autoridad que tenga que ver con la materia, dará a conocer a la comunidad dentro del plazo de seis meses las técnicas idóneas que los usuarios de los servicios de Internet

---

papel de los medios de comunicación de masas, no debe limitarse al simple hecho de suministrar información relativa a los sucesos y acontecimientos sociales, o bien permitir a los ciudadanos y. a los grupos de interés hacer valer sus argumentos y sus puntos de vista. Los medios de comunicación han de desempeñar también un importante papel formador en el seno de la sociedad. Los medios de comunicación son responsables de formar (no sólo informar) a los ciudadanos en sus concepciones, creencias e incluso en los lenguajes -visuales, simbólicos o verbales- utilizados por el público para comprender mejor el entorno en que viven y poder interpretarlo. Los medios de comunicación llegan hasta influenciar la forma en que concebimos nuestra propia identidad y el lugar que ocupamos en el mundo y tiene un papel fundamental en la formación de nuestra identidad cultural. Ello se colisiona con las características técnicas de Internet por ser una red mundial de computadores interconectada a través de oferentes oficializados, lo que además se contrapone a las normas de derecho que exigen soluciones en el marco de los sistemas jurídicos nacionales e internacionales. En todo caso, se trata de una materia compleja, ya que cualquier reflexión sobre una política general en materia audiovisual debe partir con el reconocimiento del papel específico que los medios de comunicación juegan en nuestras sociedades y la necesidad de asegurar un equilibrio entre el juego de las fuerzas del mercado y la protección del interés general. La libertad de informar tiene su límite natural en el respeto a los derechos con reconocimiento constitucional y legal y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia. Por ello su ejercicio entraña deberes y responsabilidades, y podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, que constituyan medidas necesarias en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial. (subrayado es mío).

pueden usar voluntariamente para filtrar o controlar el contenido de los programas difundidos a través de las redes señaladas".[231]

De este proyecto se pueden hacer las siguientes observaciones. En cuanto al artículo primero, se sanciona a quien difunda o propale "informaciones, contenidos o noticias". Dentro de ellos, perfectamente puede tratarse de hechos que formen parte de la esfera íntima de las personas, y que se trate de atentados contra el derecho a la vida privada y que obviamente se vuelven contrarios a la moral o a las buenas costumbres.

Este artículo también es bastante amplio en el sentido de que se aplica a "redes y procedimientos de Internet, o de otros servicios de igual naturaleza", por lo cual se ha abierto la puerta frente a otras posibles nuevas tecnologías, y eso sin duda alguna que es un acierto.

Sin embargo, definitivamente a este proyecto le quedan por regular algunos aspectos como por ejemplo el determinar quien es efectivamente el responsable de estos hechos en la red. Por ello, en cuanto al sujeto pasivo, al hablar de "El que difunda o propale" se está dando la posibilidad de que se trate de personas que no se encuentran en el territorio chileno, y por consiguiente se vuelve muy difícil, por no decir imposible, que se sancione a éstas.

Para regular Internet se requiere hacer una serie de especificaciones técnicas y definir diversos conceptos, lo cual no se ha hecho y ni siquiera se ha definido qué debe entenderse por redes y procedimientos de Internet.

Otra observación importante es la que consta en el Oficio de la Corte Suprema durante el proceso de tramitación de este proyecto, en el cual se señala la "conveniencia de precisar más el concepto de "Juez de Policía Local correspondiente", a que se refiere el artículo 2°, atendiendo los servicios de Internet, muchos de los cuales pertenecen a informaciones provenientes de otros países, como asimismo, corregir la anomalía que significa que por el artículo 2° se determine que aquel Juez será competente para conocer de las infracciones definidas en el artículo 1°, pero nada se establece respecto de la competencia para conocer de la conducta contravencional definida en el artículo 4° el proyecto". [232] De ello se desprende que este proyecto tiene todavía mucho camino por recorrer.

2.- Proyecto de Ley de Protección Civil del Honor y de la Intimidad de las Personas:

Este proyecto, básicamente destinado a proteger el honor y la intimidad de las personas desde un punto de vista civil presenta el siguiente texto:

"Título I

[231] Proyecto de Ley sobre Regulación de Internet, actualmente en tramitación en el Congreso.

[232] Oficio de la Excelentísima Corte Suprema al Congreso Nacional con fecha miércoles 3 de noviembre de 1999, en sesión 10°.

NORMAS GENERALES:

Artículo 1°.- Los derechos constitucionales al honor y a la intimidad, prescritos en los números 4° y 5° del artículo 19 de la Constitución Política, serán protegidos civilmente frente a todo género de intromisiones ilegítimas, de acuerdo con lo establecido por la presente ley.

Artículo 2 .- Las regulaciones de esta ley no obstan al ejercicio de las acciones penales por los delitos que pueden cometerse con ocasión de las intromisiones ilegítimas.

Artículo 3°.- La protección civil del honor y de la intimidad quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia.

Artículo 4° .- No se entenderá que exista intromisión ilegítima en el ámbito protegido, cuando estuviese expresamente autorizada por la ley o cuando el titular del derecho hubiese otorgado al efecto su consentimiento expreso.

El consentimiento a que se refiere el inciso anterior será revocable en cualquier momento, pero habrán de indemnizar en su caso, los daños y perjuicios causados.

El consentimiento de los menores e incapaces se sujetará a las reglas generales de la legislación civil.

Artículo 5°.- El ejercicio de las acciones de protección civil del honor y de la intimidad de una persona fallecida corresponderá al cónyuge, los descendientes, ascendientes y hermanos de la persona afectada, que viviesen al tiempo de su fallecimiento.

Con todo, la persona afectada podrá designar en su testamento a una persona natural o jurídica para que ejerza las acciones señaladas en el inciso anterior.

Artículo 6°.- Cuando sobrevivan varios parientes de los señalados en el inciso 1° del artículo anterior, cualquiera de ellos podrá ejercer las acciones previstas para la protección de los derechos del fallecido.

La misma regla se aplicará, salvo disposición en contrario del fallecido, cuando hayan sido varias las personas designadas en el testamento.

Artículo 7°.- Cuando el titular del derecho lesionado fallezca sin haber podido ejercitar, por sí o por su representante legal, las acciones previstas en esta ley, por las circunstancias en que la lesión se produjo, las referidas acciones podrán ejercitarse por las personas señaladas en el artículo 5°.

Las mismas personas podrán continuar la acción ya entablada por el titular del derecho lesionado cuando falleciese.

Título II

DE LA PROTECCIÓN CIVIL DEL HONOR Y DE LA INTIMIDAD

Artículo 8°.- Se considerarán intromisiones ilegítimas en el ámbito de protección delimitado por los artículos 3° y 4° previstos en esta ley:

a) El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.
b) La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción.
c) La divulgación de hechos relativos a la vida privada de una persona o familia, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.
d) La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela.
e) La captación, reproducción o publicación por fotografía, filme o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo 10.
f) La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.
g) La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.
h) Todo procedimiento o utilización de mecanismos o medios análogos a los anteriores.

Artículo 9°.- No se reputarán, con carácter general, intromisiones ilegítimas a la intimidad las actuaciones autorizadas o acordadas por la autoridad judicial competente de acuerdo con la ley. Tampoco se reputarán, con carácter general, intromisiones ilegítimas a los derechos de honor e intimidad las actuaciones en que exista un interés predominante de carácter histórico, científico, cultural, político o social.
Artículo 10°.- El derecho a la propia imagen no impedirá:

a) Su captación, reproducción o publicación por cualquier medio cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto o en lugares abiertos al público.
b) La utilización de la caricatura de dichas personas, de acuerdo con el uso social.
c) La información gráfica sobre un suceso o acaecimiento público, cuando la imagen de una persona determinada aparezca como meramente accesoria.

Las excepciones contempladas en las letras a) y b) no serán de aplicación respecto de las autoridades o personas que desempeñen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza.

Artículo 11 °.- Será competente para conocer de las causas que se promuevan por intromisiones ilegítimas a los derechos al honor ya la intimidad, el juez de letras en lo civil del domicilio del afectado.
En los casos en que el juez competente corresponda a lugares de asiento de Corte, en que ejerza jurisdicción civil más de un juez letrado, deberá cumplirse con lo dispuesto en el artículo 176 del Código Orgánico de Tribunales.

Artículo 12°.- Las causas a que se refiere el artículo anterior se tramitarán conforme al procedimiento sumario. En cualquier estado del juicio el juez podrá adoptar todas las medidas necesarias para poner fin a la intromisión ilegítima de que se trate y restablecer al perjudicado en el pleno disfrute de sus derechos, así como para prevenir o impedir intromisiones ulteriores. Entre dichas medidas podrán incluirse las cautelares encaminadas al cese inmediato de la intromisión ilegítima, así como el reconocimiento del derecho a replicar, la difusión de la sentencia y la condena a indemnizar los perjuicios causados.

Artículo 13°.- La existencia de perjuicios se presumirá siempre que se acredite la intromisión ilegítima. La indemnización se extenderá al daño moral que se valorará atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente producida, para lo que se tendrá en cuenta, en su caso, la difusión o audiencia del medio a través del que se haya producido. También se valorará el beneficio que haya obtenido el causante de la lesión como consecuencia de la misma.

Artículo 14°.- El importe de la indemnización por el daño moral, en el caso del artículo 5°, corresponderá a los causahabientes en la proporción en que la sentencia estime que han sido afectados y, en su defecto, a las personas designadas en el testamento. En los casos del artículo 7°, la indemnización se entenderá comprendida en la herencia del perjudicado.

Artículo 15°.- Las acciones de protección frente a las intromisiones ilegítimas prescribirán transcurridos dos años desde que el legitimado pudo ejercitarlas.

Artículo 16°.- Las disposiciones anteriores se aplicarán, en su caso, a las intromisiones ilegítimas, respecto de la reputación de las personas jurídicas."

Resulta interesante que se presente un proyecto de ley para llenar el vacío legal existente, al no contemplarse en el actual ordenamiento jurídico chileno una adecuada protección civil a la vida privada y la intimidad de las personas. Como bien lo indica el artículo primero de este proyecto, "serán protegidos civilmente frente a todo género de intromisiones ilegítimas", por consiguiente, de ello se desprende que las intromisiones hechas a través de Internet deben estar contempladas.

También se regula al respecto de la vida privada de las personas fallecidas, por lo que se confirma la intención del legislador por proteger no solo a la intimidad de quienes han muerto, sino de ampliar este resguardo también a sus familiares.

El Título II de este proyecto en su artículo octavo enumera diferentes maneras de intrometerse ilegítimamente en la intimidad de las personas. Dentro de las maneras que esta ley contempla, muchas pueden realizarse a través del uso de Internet.

En cuanto a la competencia de los tribunales sobre los hechos que pretende proteger esta norma, constituida en el artículo 11°, proceden hacerse las mismas observaciones que se hicieron respecto del proyecto de ley anterior.

Por último, resulta interesante constatar que este proyecto, en el artículo 16°, protege las intromisiones ilegítimas que afecten la reputación de las personas jurídicas.

Segunda Parte

Intimidad y Tecnología

CAPITULO IV: INTERNET Y LOS NUEVOS MEDIOS ELECTRÓNICOS

En menos de diez años, el hombre ha sufrido transformaciones sustanciales y de hecho, seguramente, nunca la vida cotidiana de las personas ha tenido tantos cambios en tan poco tiempo en la historia de la humanidad por causa de las tecnologías. Esto se ha visto reflejada en distintos ámbitos, pero sin duda que uno de los más trascendentales ha sido el de las telecomunicaciones. Bill Gates, en una carta dirigida al Gobierno de los Estados Unidos decía que "Cuando una nueva tecnología emerge con el potencial de cambiar la forma en que la gente vive y trabaja, también genera un vivo debate acerca de su impacto en nuestro mundo, y preocupación sobre la forma en que debe ser adoptada"[233]. Por dar un ejemplo, a principios de los noventa, el teléfono celular prácticamente no existía entre las sociedades latinoamericanas, mientras que en la actualidad, difícilmente un profesional se atrevería a salir a trabajar sin este novedoso aparato, y el olvidarlo podría traducirse hasta en una catástrofe profesional o familiar... Y es que el avance de la tecnología es tal que comprarse un teléfono celular resulta arriesgarse a que en poco tiempo quede obsoleto.

En el ámbito computacional, la historia no es menos elocuente. ¿Desde hace cuanto tiempo que escuchamos hablar de términos como Internet, mensajes electrónicos, conexión de banda ancha o chat (términos que hace unos pocos años no nos decían nada y ahora hasta las generaciones más pequeñas los conocen) por apenas dar algunos ejemplos? El tiempo promedio que las personas en la actualidad pasan frente a un computador ha aumentado considerablemente con la llegada de las llamadas *nuevas tecnologías*. Ya en la actualidad aquel que no sabe manejar este nuevo medio de comunicación llamado "Internet", o aquel que no tiene una dirección de correo electrónico, prácticamente podríamos decir que se encuentra un poco retrasado en el tiempo. Retomando las palabras del propio Gates, "como el teléfono, la electricidad, el automóvil o el aeroplano delinearon nuestro mundo en el siglo XX, Internet dará forma a los primeros años del siglo XXI y tendrá un profundo y positivo impacto en la forma en que trabajamos y vivimos"[234].

A continuación, en busca de una introducción suficiente para comprender esta poderosa herramienta de comunicación, procederé a hacer una breve descripción de lo que son Internet y otros medios electrónicos.

Breve Introducción de Internet:

Durante la Guerra Fría, el desarrollo militar y tecnológico en los países capitalistas y comunistas trajo consigo interesantes adelantos. Es así que la historia de Internet se remonta al año 1969, fecha en que la *Advanced Research Projects Agency*, más conocida como ARPA[235] (antigua DARPA[236]), pretendía conectar

[233]William H. GATES, Ensayo para el Presidente de Estados Unidos, texto publicado de www.emol.cl con fecha 8 de febrero de 2001, visitado por el autor de este trabajo en la misma fecha.

[234] Ibídem.

[235] Según el Glosario de Términos Informáticos, es *Advanced Research Projects Agency* o ARPA (Agencia de Proyectos de Investigación Avanzada) el nombre actual del organismo militar norteamericano anteriormente llamado DARPA,

una serie de cuatro computadores, ubicados todos ellos en universidades del suroeste de los Estados Unidos. El objetivo era diseñar una red comunicacional que pudiese resistir un eventual ataque nuclear, de tal manera que si la ruta principal entre dos puntos era destruida, los "enrutadores" o *routers*[237] pudieran proporcionar rutas alternativas. Con el tiempo, lo que comenzó como una simple conexión de computadores entre organismos militares se fue ampliando a nivel de universidades y entidades científicas. Sin embargo, al ser un sistema bastante precario y difícil de utilizar, su uso masivo no progresó.

A principios de los años setenta, el desarrollo de la red dio un paso importante al incorporarse los llamados protocolos *TCP/IP*[238] o Protocolo de Control de Transmisión / Protocolo Internet, que ya para el año 1983 estaban repartidos universalmente. Más tarde se implementarían nuevos sistemas como el *UUCP* o UNIX-to-UNIX CoPy (Copia de UNIX a UNIX) que inicialmente se trataba de un programa que se procesaba en el sistema operativo UNIX y que permitía a un sistema UNIX enviar ficheros a otro sistema UNIX a través de la línea telefónica. Después se utilizó sobre todo para describir la red internacional que utilizaba el protocolo UUCP para enviar noticias y correo electrónico. Hoy está en desuso. [239] Este sistema daría origen a la llamada "red de los newgroups". Más tarde se crearía la *BITNET* , Because It´s Time NETwork (Red Porque Ya Es Hora), antigua red internacional de ordenadores de centros docentes y de investigación que ofrecía servicios interactivos de correo electrónico y de transferencia de ficheros utilizando un protocolo de almacenaje y envío basado en los protocolos Network Job Entry de IBM. Se conectaba a Internet a través de una pasarela de correo electrónico.

---

dedicado a desarrollar proyectos de investigación con propósitos militares que a veces tienen también utilización civil. Definición obtenida en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[236] Se entiende por *Defense Advanced Research Projects Agency* o DARPA (Agencia de Proyectos de Investigación Avanzada para la Defensa) Organismo creado en 1954 por el Departamento de Defensa norteamericano (DoD) encargado de la investigación y desarrollo en el campo militar y que jugó un papel muy importante en el nacimiento de Internet a través de la red ARPANET. Definición obtenida de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[237] Se define a *router* (encaminador,direccionador,*enrutador*) como el dispositivo que distribuye tráfico entre redes. La decisión sobre a donde enviar los datos se realiza en base a información de nivel de red y tablas de direccionamiento. Definición obtenida de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[238] La definición de este concepto es la siguiente: "*Transmission Control Protocol/Internet Protocol* o TCP/IP (Protocolo de Control de Transmisión/Protocolo Internet) Sistema de protocolos, definidos en RFC 793, en los que se basa buena parte de Internet. El primero se encarga de dividir la información en paquetes en origen, para luego recomponerla en destino, mientras que el segundo se responsabiliza de dirigirla adecuadamente a través de la red". Por su parte, debe entenderse a *RFC* o *Request For Comments* o RFC (Petición de Comentarios) como una "serie de documentos iniciada en 1967 que describe el conjunto de protocolos de Internet y experimentos similares. No todos los RFC's (en realidad muy pocos de ellos) describen estándares de Internet pero todos los estándares Internet están escritos en forma de RFC's. La serie de documentos RFC es inusual en cuanto los protocolos que describen son elaborados por la comunidad Internet que desarrolla e investiga, en contraste con los protocolos revisados y estandarizados formalmente que son promovidos por organizaciones como CCITT y ANSI". Definiciones obtenidas de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[239] Ver mas sobre este término en el Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

Con ello también se fueron desarrollando los comandos para el *electronic mail* (e-mail)[240] o correo electrónico, el *Federal Transfer Protocol* o FTP (Protocolo de Transferencias de Ficheros)[241] y el protocolo *Telnet* al que se le conoce como un protocolo estándar de Internet para realizar un servicio de conexión desde un terminal remoto (en la actualidad casi no tiene uso).

Las consecuencias de estos importantes avances facilitaron considerablemente el uso de la red, lo cual permitió que este nuevo medio de comunicación se expanda mayormente a través de bibliotecas y medios universitarios. A esas alturas, Internet no tenía sino un puñado de usuarios, por lo cual controlar la red y su expansión no presentaba mayor dificultad. Sin embargo, esto duró poco ya que a finales de los años ochenta, la necesidad de elaborar medios que permitieran un adecuado esparcimiento de la red llevaron a la creación del sistema *Archie*[242] en 1989. Periódicamente, se fueron conectando a todos los servidores de FTP conocidos, obteniendo de esta manera un listado de ficheros disponibles en dichos servidores.

Más tarde se crearía el *WAIS,* Wide Area Information Servers (Servidores de Información de Área Amplia), que es un servicio de información distribuida, anterior al *WWW,* y que permitía hacer preguntas en lenguaje simple, la búsqueda indexada para obtener información con rapidez y un mecanismo de retroalimentación de información relevante para lograr que los resultados de una búsqueda inicial repercutiesen en búsquedas subsiguientes.[243] No obstante, el sistema todavía era un tanto complicado.

En 1991 apareció un programa llamado *Gopher*[244], que a grandes rasgos consistía en un sistema de menús para acceder a ficheros. Su éxito fue inmediato y al poco tiempo había más de 10.000 *Gophers* interconectados alrededor de todo el mundo. A su vez, con la creación de una herramienta llamada

---

[240] Se define a este concepto como "Aplicación mediante la cual un ordenador puede intercambiar mensajes con otros usuarios de ordenadores (o grupos de usuarios) a través de la red. El correo electrónico es uno de los usos más populares de Internet. Dícese también de los mensajes enviados a través de este medio." Definición obtenida de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[241] *File Transfer Protocol* o FTP (Protocolo de Transferencia de Ficheros) es el protocolo que permite a un usuario de un sistema acceder a, y transferir desde, otro sistema de una red. FTP es también habitualmente el nombre del programa que el usuario invoca para ejecutar el protocolo. Definición obtenida de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[242] Se define a *Archie* como una "aplicación ya obsoleta, anterior al WWW, cuyo objetivo era recoger, indexar y servir información dentro de Internet automáticamente", definición de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[243] Definición obtenida de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[244] Se entiende por *Gopher* (Gopher) al "antiguo servicio de información distribuida, anterior a la aparición del WWW. Desarrollado por la Universidad de Minnesota, ofrecía colecciones jerarquizadas de información en Internet". Definición de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

VERÓNICA (un programa que recorría diferentes *Gophers* del mundo recopilando enlaces y construyendo índices), la utilidad del *Gopher* aumentó[245].

Por su parte, el *CERN*[246] o *Conseil Européen pour la Recherche Nucléaire* (Consejo Europeo para la Investigación Nuclear) , en 1991 daba el paso más importante en la historia del desarrollo de Internet: la creación de un nuevo protocolo del cual nacería la *WWW*[247] o *World Wide Web* o *W3* (Telaraña Mundial, Malla Mundial o Red Mundial) que a grandes rasgos consiste en un sistema basado en el hipertexto[248] (en inglés hypertext), que es una forma de conectar unos textos con otros a base de incluir enlaces entre ellos. A pesar de que fue un programa sumamente costoso, en 1993 comenzó su despegue. Ese mismo año se creó el primer "programa cliente" o *navegador* (navigator) o *browser*[249]. Ello fue fundamental para la utilización de lo que se conoce como el progama *Mosaic*[250], indispensable para el despegue de lo que serían los programas que permitan a los usuarios "navegar" en la red. En 1992, *Delphi* sería la primera empresa privada en ofrecer acceso a Internet, destruyendo cualquier intención de limitar su uso exclusivamente con un fin económico.

---

[245] Se dice que un sistema parecido fue el *JUGHEAD*, que tendría similares características que el sistema *VERÓNICA*. Información obtenida en http://www.simil.com/casdeiro/internet/hist.htm por Manuel Casal Lodeiro.

[246] El *Conseil Européen pour la Recherche Nucleaire* o *CERN* (Consejo Europeo para la Investigación Nuclear) es una institución europea, creada en 1954 y situada en Ginebra, Suiza, que desarrolló, para sus necesidades internas, el primer navegador y el primer servidor WWW (proyecto liderado por Tim Berners-Lee). Ha contribuido decisivamente a la difusión de esta tecnología y es uno de los rectores del W3 Consortium, el organismo clave en la difusión y estandarización de WWW. Información obtenida del Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[247]Se define a *World Wide Web* o *WWW* o *W3* (Malla Mundial,Telaraña Mundial,*WWW*) como un "sistema de información distribuido, basado en hipertexto, creado a principios de los años 90 por Tim Berners-Lee, investigador en el CERN, Suiza. La información puede ser de cualquier formato (texto, gráfico, audio, imagen fija o en movimiento) y es fácilmente accesible a los usuarios mediante los programas navegadores. Es preciso destacar el hecho poco habitual de que tanto Berners-Lee como el CERN renunciaron a la explotación comercial de este extraordinario invento." Definición obtenida del Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[248]De las definiciones del Glosario de Términos Informáticos, es prudente revisar las siguientes con el objeto de entender mejor el desarrollo de Internet: "*hypertex*t (hipertexto): Aunque el concepto en sí es muy anterior al WWW (fue creado por el físico norteamericano Vannevar Bush en 1945), en Internet el término se aplica a los enlaces existentes en las páginas escritas en HTML, enlaces que llevan a otras páginas que pueden ser a su vez páginas de hipertexto. Las páginas hipertextuales son accedidas normalmente a través de navegadores WWW; *HyperText Markup Language* o HTML (Lenguaje de Marcado de Hipertexto): Lenguaje en el que se escriben las páginas a las que se accede a través de navegadores WWW; *HyperText Transfer Protocol* o HTTP (Protocolo de Transferencia de Hipertexto): Protocolo usado para la transferencia de documentos WWW". En http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[249] Se entenderá por *browser* (visor, visualizador,hojeador,*navegador*) a la "aplicación para visualizar todo tipo de información y navegar por el espacio Internet. En su forma más básica son aplicaciones hipertexto que facilitan la navegación por los servidores de información Internet; cuentan con funcionalidades plenamente multimedia y permiten indistintamente la navegación por servidores WWW, FTP, Gopher, el acceso a grupos de noticias, la gestión del correo electrónico, etc". Definición obtenida del Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[250] Se entiende por *Mosaic* (Mosaic) al "navegador WWW promovido por la NCSA en 1993 y desarrollado por Marc Andreessen, más tarde fundador de la empresa Netscape. Fue el primero que tuvo funcionalidades multimedia y sentó las bases del modelo de publicación y difusión WWW". Definición obtenida del Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

En poco tiempo, muchos proveedores de servicio de Internet aparecieron en Estados unidos y el resto del mundo, dando pie a un despegue espectacular de la red.

A mediados de los noventa, lo que era anteriormente un proyecto fundado por el Gobierno norteamericano para su uso exclusivo y de ciertos privilegiados, abrió sus fronteras al mundo y en poco tiempo se convertiría en el medio de comunicación más poderoso y sofisticado, capaz de transmitir texto, imágenes y sonido sólo en segundos. El desarrollo de Internet se manifiesta día a día, casi violentamente, y lo que antes era un medio de comunicación computacional, ahora se está transformando en una herramienta utilizada en la telefonía, a través de agendas electrónicas o en automóviles, por apenas dar simples ejemplos que ahora se conocen.

En busca de una definición de Internet:

Resulta un tanto complicado para la doctrina dar una definición de Internet cabal y completa. Ya algunos científicos, sistemas legislativos e incluso judiciales se han aventurado por tratar de definir a la red. A continuación, algunas de estas propuestas:

El Glosario de Términos Informáticos, en http://www.ati.es/novatica/glosario/glosario_internet.html, hace una primera distinción, señalando que: "internet (con "i" minúscula) es un conjunto de redes conectadas entre sí". Por otro lado, "Internet (La Red, *Internet*) es la Red de telecomunicaciones nacida en 1969 en los EE.UU. a la cual están conectadas centenares de millones de personas, organismos y empresas en todo el mundo, mayoritariamente en los países más desarrollados, y cuyo rápido desarrollo está teniendo importantes efectos sociales, económicos y culturales, convirtiéndose de esta manera en uno de los medios más influyentes de la llamada Sociedad de la Información y en la Autopista de la Información por excelencia. Fue conocida como ARPANET hasta 1974."[251]

Dentro de la doctrina española, la página electrónica Informática Milenium define a Internet de la siguiente manera: "El Internet, algunas veces llamado simplemente "La Red", es un sistema mundial de redes de computadoras, un conjunto integrado por las diferentes redes de cada país del mundo, por medio del cual un usuario en cualquier computadora puede, en caso de contar con los permisos apropiados, accesar información de otra computadora y poder tener inclusive comunicación directa con otros usuarios en otras computadoras."[252]

La página web española "bogote" dice que: "Internet es una gran red de redes que une a computadoras en más de 160 países en distintas partes del mundo. Para entender mejor la definición de Internet, debemos empezar sabiendo lo que es una red. Una red es un conjunto de computadoras y dispositivos periféricos unidos por medio de un canal de comunicaciones con el fin de compartir recursos. Internet es una red que une a estas

[251] Definición obtenida del Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[252] Información obtenida en http://www.informaticamilenium.com.mx/Paginas/espanol/sitioweb.htm, visitada en marzo del 2002.

redes, y es por eso que se le da la denominación de RED DE REDES. No es posible calcular con exactitud la cantidad de usuarios que están interconectados, ya que cada día hay más personas que se unen a esta red."[253]

En las Jornadas Españolas de Documentación se buscó lograr mayor precisión a la hora de utilizar el vocablo "Internet", distinguiendo los siguientes términos: "se denominaría a 'Internet invisible' o Infranet al conjunto de recursos accesibles únicamente a través de algún tipo de pasarela o formulario Web y que, por tanto, no pueden ser indizados de forma estructural por los robots de los buscadores. Desde un punto de vista documental se distinguen cuatro grandes categorías en la infranet: a) Catálogos de bibliotecas y bases de datos bibliográficas. Los OPAC y las bases de datos de registros bibliográficos accesibles a través de pasarelas web resultan imposibles de interrogar exhaustivamente por los motores convencionales. b) Bases de datos. Se incluyen todas las bases de datos no bibliográficas, con un amplio abanico de tipologías, desde las bases alfanuméricas o a texto completo hasta las obras de referencia, tipo diccionario o enciclopedia. c) Revistas electrónicas y archivos de documentos. Tanto las de acceso gratuito, pero que exigen registro previo, como las de pago protegidas por palabra clave son invisibles a los motores. Añádanse las que solo o recen la recuperación de sus artículos mediante búsqueda y no utilizan navegación por sumarios de contenidos. d) Depósitos y documentos en formatos no indizables." [254]

Una interesante definición es la del Instituto Tecnológico de Santo Domingo, que dice que: "Intemet es la red global de computadoras que nos permite acceso a una vasta cantidad de información a través de múltiples servicios. Internet es una "red de redes" que conecta un sinnúmero de máquinas y redes de diferentes tecnologías. Su nombre es una apropiación del término Internet que en inglés computacional designa a la conexión entre muchas redes. Eso es Internet, una serie de redes institucionales (en buena medida académicas) de diversas arquitecturas, interconectadas por un protocolo común conocido como TCP/IP".[255]

Una de las definiciones célebres es la que dio el 24 de octubre de 1995, el *Federal Networking Council*, FNC de los Estados Unidos, que aprobó unánimemente una resolución definiendo en uno de sus partes a este término. Esta definición se desarrolló en consultas con los principales líderes de Internet y las *Intellectual Property Rights (IPR) Communities*. Esta resolución, de traducción no oficial, recuerda que:

"El *Federal Networking Council* (FNC) acuerda que el siguiente lenguaje refleja nuestra definición del término "Internet".

"Internet" se refiere al sistema global de información que :

1.- está lógicamente unido por un espacio global único de dirección basado en el protocolo de Internet TCP/IP o sus extensiones/continuaciones subsecuentes;

[253] Definición obtenida en http://www.bogote.com/infob/b-net.ht , visitada en marzo del 2002.

[254] Información obtenida en http://dois.mimas.ac.uk/DoIS/data/Papers/julmjoifp3964.html, visitada en marzo de 2002.

[255] Información obtenida en http://www.intec.edu.do/redintec/manual_internet/internet.html, visitada en marzo de 2002.

2.- es capaz de soportar comunicaciones usando la serie de protocolos Transmission Control Protocol/Internet Protocol (TCP/IP) y sus extensiones/continuaciones subsecuentes; y/o otros protocolos IP-compatibles; y

3.- ofrece, usa o hace accesibles, ya sea pública o privadamente, servicios de alto nivel soportados en las comunicaciones e infraestructura relacionada descrita aquí."[256]

Dentro de la jurisprudencia chilena, en la sentencia que rechazaba un recurso de protección contra ENTEL, en el considerando 17° la Corte de Apelaciones de Concepción se redactaron las siguientes definiciones:

"Considerando 17° Que la "Red" es cualquier sistema que conecta ordenadores, con el fin de permitir el acceso común a los recursos de los demás elementos que la integran.

Que definiendo Internet puede decirse que es la red de redes o colección de redes entrelazadas. Más concretamente, como una red mundial de computadores interconectada a través de oferentes oficializados o un sistema de redes de computadores que permite el intercambio de información."[257]

Características de Internet:

1.- Internet es un medio de comunicación: Dentro de la doctrina hay pleno acuerdo respecto de esta característica. Sin embargo, existe un interesante debate sobre si Internet podría o no calificarse como un "medio de comunicación **social**". El ordenamiento jurídico chileno, en la Ley 19.733 sobre Libertades de Opinión e Información dice que:

"Artículo 2°.- Para todos los efectos legales, son medios de comunicación social aquellos aptos para transmitir, divulgar, difundir o propagar, en forma estable y periódica textos, sonidos o imágenes destinados al público, cualesquiera el soporte o instrumento utilizado.

Se entenderá por diario todo periódico que se publique a lo menos cuatro días en cada semana y cumpla con los demás requisitos establecidos por la ley."[258]

Más adelante, el Título III de esta ley, refiriéndose a las formalidades de funcionamiento de los medios de comunicación social, señala que:

"Artículo 9°.- En los casos en que la ley permita que el propietario de un medio de comunicación social sea una persona natural, ésta deberá tener domicilio en el país y no haber sido condenada por delito que merezca pena aflictiva. Tratándose de personas jurídicas, éstas deberán tener domicilio en Chile y estar constituidas en el país o tener agencia autorizada para operar en el territorio nacional. Su presidente y sus

[256] Ibídem.

[257] Considerando 17° del Recurso de Protección N°243-1999 contra ENTEL Chile, en Del Archivo de Gaceta Jurídica, N° 239, pág. 228, edición de Mayo del 2000, Santiago, Chile.

[258] Artículo segundo de la Ley 19.733 sobre Libertades de Opinión e Información y Ejercicio del Periodismo.

administradores o representantes legales deberán ser chilenos y no haber sido condenados por delito que merezca pena aflictiva (...).

Artículo 10°.- Los medios de comunicación social deberán tener un director responsable y, a lo menos, una persona que lo reemplace.

El director y quienes lo reemplacen deberán ser chilenos, tener domicilio y residencia en el país, no tener fuero, estar en pleno goce de sus derechos civiles y políticos, no haber sido condenado por delitos que merezcan pena aflictiva y en los últimos dos años, no haber sido condenado como autores de delitos reiterados o como reincidentes en delitos penados por la ley (...).

Artículo 11°.- Los medios de comunicación social podrán iniciar sus actividades una vez que hayan cumplido con las exigencias de los artículos anteriores.(...)"[259]

Analizando detalladamente los artículo recién expuestos, se puede concluir que para que esta ley sea aplicable a Internet, se requerirá a grandes rasgos que este medio de comunicación esté domiciliado en el territorio chileno, que tenga un presidente, administradores, representantes legales, tener un director responsable, etc...

Como bien lo señala Jijena Leiva, "en Internet no existe un editor o un director responsable contra quien dirigirse, por ejemplo si empiezan a circular mensajes antiracistas, neofazistas, avisos de servicios sexuales, etc. A mayor abundamiento: para la prensa escrita Internet constituye solamente una nueva forma –digital y virtual- de difundirse, pero las responsabilidades de lo que en sus páginas WEB se diga o informe siempre serán imputable al periodista, editor o director de un específico medio de prensa, de la misma manera que lo sería en base a la publicación del diario en soporte papel".[260]

Así mismo, la propia jurisprudencia chilena, en la sentencia del ya citado caso ENTEL señalaba que: "Considerando 17° Se sostiene que Internet es un "medio de comunicación" basado en la libertad para la circulación de la información. En cambio, para otros es un "medio de transporte de información", porque aquí fluye información de todo tipo, que no se genera en el medio, como en la radio o la televisión, sino que hay información de todo el mundo.

La red Internet se caracteriza por no tener dueño ni gerente ni representante legal, por ser de alcance mundial y de acceso general."[261]

---

[259] Ibídem, artículo noveno décimo y undécimo.

[260] Renato JIJENA LEIVA, "Internet, privacidad y derecho, un desafío de cara al siglo XXI en el marco de la globalización", pág. 2 de texto publicado en http://vlex.com/redi/No._36_-_Julio_del_2001/3, visitado en enero de 2002.

[261] Recurso de Protección N°243-1999 contra ENTEL Chile, en Del Archivo de Gaceta Jurídica, N° 239, pág. 228, edición de Mayo del 2000, Santiago, Chile.

De lo anteriormente expuesto se puede concluir que para el ordenamiento jurídico y para la jurisprudencia chilenos, Internet no puede considerarse como un medio de comunicación *social* y por consiguiente no puede aplicársele la Ley 19.733 ni menos el artículo 19 N°4, inciso segundo del Código Político. La única excepción al respecto es para quienes hagan uso de Internet y sean medios de comunicación social que utilicen este medio de difusión a través de su página web, como por ejemplo la página electrónica del diario El Mercurio, que sí tiene editores, y autoridades que son responsables de los actos cometidos a través de este medio "complementario" de su actividad principal como medio de comunicación escrito de libre circulación.

Pero, es perfectamente aplicable a Internet tanto los numerales cuarto inciso primero y quinto del artículo 19. Si bien no existen en la actualidad normas específicas que regulen Internet, no por ello se debe descartar que se apliquen normas análogas para otros medios de comunicación, y desde este punto de vista, criterios que se apliquen por ejemplo para censurar diarios o revistas o medios televisivos, deberían servir de parámetro a la hora de regular Internet. Claro que, a diferencia de otros medios de comunicación, las características de la red imposibilitan que se proceda de igual manera que frente a los otras vías de información. Para ello, deben los tribunales buscar otras salidas análogas de presentarse irregularidades, dentro de lo posible.

Definitivamente Internet es un medio de comunicación, pero no social, sino que es un "medio de comunicación masiva"[262] como se le llama en el Proyecto de Ley Sobre Regulación de Internet. Otros como Humberto Carrasco Blanc creen que "es un medio tecnológico que permite a diversos actores comunicarse con diversos fines".[263]

2.- Internet es a-territorial: no existe un lugar físico en el cual se encuentre materialmente Internet, pues como se indicaba anteriormente, la red se encuentra en un lugar o espacio virtual, también llamado "ciberespacio"[264], conformado por millones de computadores conectados entre sí. Internet no es una entidad física ni menos tangible.

3.- Internet es a-gubernamental: no hay un gobierno de la red. Tampoco una institución que se encargue de regular el funcionamiento de Internet a nivel mundial, o que por lo menos tenga un reconocimiento internacional. Ninguna entidad, ni académica, corporativa, militar, o con fines de lucro administra este medio

---

[262] Este proyecto de ley sobre Regulación de Internet, presentado por los diputados señores Velasco, Villouta, Krauss, Jarpa, Núñez, Patricio Cornejo, Vilches, Olivares, Ceroni y Reyes en boletín N° 2395-19, en parte del discurso señalaba que:"...en un Estado de derecho los medios de comunicación masiva deben observar deberes y responsabilidades específicas para quienes se desempeñan en estos organismos. Esta situación que es más obvia tratándose de los medios tradicionales, es decir prensa escrita, radio y televisión, se alteran cuando se trata de defender los derechos en medios electrónicos como la Internet(...)". El discurso completo se encuentra en la nota 230 del capítulo anterior.

[263] Humberto CARRASCO BLANC, Chile: Algunos Aspectos de la Responsabilidad de los Proveedores de Servicio y Contenidos de Internet. El caso ENTEL, pág. 4, de texto publicado en http://vlex.com/redi/No._26_-_Septiembre_del_2000/4, visitado en enero de 2002.

[264]Se define a *Cyberspace* (Ciberespacio) como un "término creado por William Gibson en su novela fantástica "Neuromancer", del año 1984 para describir el 'mundo' de los ordenadores y la sociedad creada en torno a ellos". Definición obtenida del Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

de comunicación. Por consiguiente, no hay editores, directores o entes que se encarguen de controlar su adecuado funcionamiento a nivel mundial. Desde esta perspectiva, la autorregulación ha sido, sobre todo en los inicios de Internet, una solución viable para enfrentar este régimen casi "anarquista". El propio Bill Gates, en una carta dirigida al Presidente de los Estados Unidos a principios del año 2001 manifestaba que: "Internet ha evolucionado hacia un intercambio informativo único e independiente, capaz de crecer orgánicamente, que puede operar en forma confiable con una gestión poco centralizada y que está construida por completo con base en normas comunes. Son esas normas comunes las que han ayudado a hacer tan exitosa la Internet. Desde el TCP/IP, el protocolo que es como el "guardián del tráfico" de datos en Internet, al HTML y XML, los lenguajes del World Wide Web (www), las normas comunes han abierto Internet "a cualquiera que hable su idioma"."[265]Sin embargo, en la actualidad, esta postura se cuestiona ya que el inmesurable crecimiento de la red no garantiza un respeto universal de su uso.

4.- Es una red de redes: se le llama popularmente a Internet la "red de redes", ya que su funcionamiento consiste en un sinnúmero de computadores conectados entre sí, que a su vez también están conectados con otros, y así sucesivamente, de tal manera que se forma una red global de computadores interconectados, todos ellos formando una gran red, conocida como Internet.

5.- Naturaleza de Internet: es tremendamente difícil, por no decir imposible, determinar el tamaño o las dimensiones de la red. Se trata del medio de comunicación que más ha crecido en la historia en tan poco tiempo, de tal manera que su desarrollo se duplica cada año. Permite por ejemplo que lugares remotos del mundo puedan sentirse conectados a cualquier mercado o bolsa de valores, empresa o persona determinada.

6.- Es un medio de comunicación completo y masivo: es un medio que cumple por sí solo las funciones que los otros medios de comunicación realizan por separado. Puede transmitir imágenes y audio, como la radio o la televisión; transmitir texto, como diarios y revistas; enviar y recibir información escrita, como el fax; transmitir voz, como el teléfono. Todo ello es posible sin necesidad de una conexión a una moderna antena o satélite especial de carácter exclusivo. De ello se desprende que es un medio de comunicación masivo, popular y económico. A este respecto, Gates señalaba que: "Grandes empresas pueden conectarse con sus empleados, proveedores y socios alrededor del mundo y los pequeños empresarios pueden encontrar a sus clientes en cualquier lugar. Los empresarios pueden además contratar empleados capacitados sin importar donde estén y expandir enormemente las oportunidades de trabajo en Estados Unidos, dando a las naciones en desarrollo la oportunidad de convertirse en economías fuertes, proveedoras de servicios de TI (Tecnologías de Información) para el resto del mundo. Internet, junto con otras tecnologías vinculadas a la computación, está literalmente facilitando a algunos países en desarrollo dar "el salto de rana" a la revolución industrial y el brinco directo hacia la Era de Internet. Internet permite a la gente estar junta y más cerca. Antes de Internet

[265] William H. GATES, Ensayo para el Presidente de Estados Unidos, texto publicado de www.emol.cl con fecha 8 de febrero de 2001.

era posible mantenerse en contacto con los familiares y amigos en distintos países del mundo, pero resultaba demasiado caro."[266]

Por ello, y en especial consideración con el objeto de estudio de este trabajo, Internet debe considerarse especialmente desde dos perspectivas:

a) como medio de transmisión de información.
b) como medio de acceso a información.

Efectivamente, se trata de una tecnología que ha cambiado y está cambiando al mundo y lo seguirá haciendo. De hecho, quienes están vinculados a la informática señalan que Internet está literalmente "en pañales". Así lo han señalado los expertos: "Internet aún está donde el automóvil estaba durante la era del modelo "T" de Henry Ford. Hemos estado viendo muchas cosas impresionantes, pero aún hay mucho más por venir. Sólo estamos al comienzo de la Era de Internet. En los próximos años, Internet tendrá un efecto aún más profundo en la forma como trabajamos, vivimos y aprendemos. Facilitando la comunicación instantánea y permitiendo el comercio en el mundo por medio de todos los dispositivos imaginables, esta tecnología será una de las llaves de las fuerzas económicas y culturales del inminente siglo XXI."[267]

Sin embargo, tenemos que ser concientes que todo desarrollo de la tecnología también trae consigo muchas cosas negativas, y su poder muchas veces puede resultar nefasto para el ser humano. Analicemos, en todo caso, otras nuevas tecnologías que están cambiando la vida del hombre.

La telefonía móvil de tercera generación:

Dentro de los grandes avances que han tenido las telecomunicaciones, es de considerar, junto con Internet, el de la telefonía celular.[268] Es así, según los expertos en el tema, que se están abriendo las puertas al "usuario de las comunicaciones móviles a la Sociedad de la Información del siglo XXI".

Haciendo una breve reseña histórica al respecto, podemos señalar que la primera generación de teléfonos móviles fueron los celulares analógicos que aparecieron a principios de los noventa en el mercado. Se trataba de un teléfono bastante precario en relación al que existe hoy en día, de mayor tamaño, más pesado, con baterías de poca duración, y con señal de corto alcance. Sin embargo, esta generación dio paso en poco

---

[266] Ibídem.
[267] William H. GATES, Ebsayo para el Presidente de Estados Unidos, texto publicado en www.emol.cl, con fecha 8 de febrero de 2001, visitada por el autor de este trabajo en la misma fecha.

[268] Se entiende por *cellular phone* (telefonino, teléfono móvil,celular,*móvil* ,teléfono celular) al "teléfono portátil sin hilos conectado a una red celular y que permite al usuario su empleo en cualquier lugar cubierto por la red. Una red celular, y los teléfonos a ella conectados, puede ser digital o analógica. Si la red es digital el teléfono puede enviar y recibir información a través de Internet." Definición obtenida del Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

tiempo a la tecnología GSM[269] o de segunda generación la cual proporciona mayor seguridad y calidad de servicio, y que permite a grandes rasgos transmisión de voz y de datos. A través de la telefonía celular ha sido posible conectarse a Internet, pero el servicio que se presta resulta un tanto insuficiente y de poco uso a nivel de los usuarios.

Por su parte, la tecnología de comunicación inalámbrica GSM evolucionó hacia la tecnología de comunicación GPRS[270] (en la práctica, esto se tradujo en una ampliación del ancho de banda, que trajo como consecuencia mayor cobertura y mayor velocidad en las comunicaciones, facilitando el acceso de Internet a través del teléfono celular).

En la actualidad se está produciendo de nuevo un cambio hacia la tercera generación de teléfonos móviles gracias a la tecnología UMTS[271], la cual ofrece nuevas dimensiones para las comunicaciones móviles, con más ancho de banda, mayor calidad y eficiencia en las prestaciones del servicio de comunicación móvil. Uno de los grandes avances en cuanto a la conexión a Internet a través del teléfono celular lo trae la llamada tecnología WAP[272], que a grandes rasgos combina las características de Internet con la de los estándares desarrollados para los terminales móviles a través de la ya citada tecnología UMTS. Esta tecnología permitirá la convergencia en el medio de distribución inalámbrico de las telecomunicaciones y los servicios de difusión o audiovisuales, además de una conexión a Internet mucho más eficiente. Se dice que la conexión a la red no dista mucho de lo que representa hacerlo a través de un computador personal, también llamado PC (o Personal Computer, pero no confundir con Partido Comunista...).

En todo caso, debe a su vez considerarse la potencial amenaza que esta nueva tecnología representa para el derecho a la vida privada de las personas, ya que nuevamente, datos sobre información que consideramos como personal pueden transmitirse a otros sin nuestro consentimiento.

---

[269] Corresponde a la siglas GSM la siguiente definición: *"Global System for Mobile communication* o GSM (Sistema Global para comunicaciones Móviles) Sistema compatible de telefonía móvil digital desarrollado en Europa con la colaboración de operadores, Administraciones Públicas y empresas. Permite la transmisión de voz y datos." Definición obtenida del Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[270] *General Packet Radio Service* o GPRS (Servicio General de Radio por Paquetes) es un "Servicio de comunicación de telefonía móvil basado en la transmisión de paquetes. Puede transmitir a una velocidad de hasta 114 Kbps y permite la conexión a Internet. Se estima que estará disponible comercialmente en el año 2001 y es una tecnología intermedia entre los sistemas GSM y UMTS." Definición obtenida del Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[271] Se entiende por *UMTS* o *Universal Mobile Telecommunications System* (Sistema Universal de Telecomunicaciones Móviles) al "estándar de telefonía móvil celular de banda ancha y alta velocidad (de 2 Mbps en adelante) desarrollado por el ETSI (European Telecommunications Standard Institute). Se trata de un sistema de tercera generación que permite la conexión a Internet. Sustituirá a los sistemas GSM y GPRS, y debería estar disponible comercialmente a partir del año 2001 o 2002." Definición obtenida del Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[272] Se define a *Wireless Application Protocol* o *WAP* (Protocolo de Aplicación de Telefonía Inalámbrica) al "protocolo que permite a los usuarios de teléfonos móviles el acceso a servidores web especializados, visualizando la información en el visor del teléfono". Definición obtenida del Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

Según palabras del español Fernando Ramos Suárez, "Con la aparición de esta nueva tecnología de comunicación inalámbrica nuestros datos personales una vez más pueden quedar afectados por el rastro que dejan al navegar por Internet. Sin embargo y a diferencia de la navegación desde el PC de casa, la navegación con el móvil tiene una serie de peculiaridades. Al estar la dirección IP de conexión a Internet vinculada a un teléfono móvil de una determinada persona, identificable por un contrato de prestación de servicios, puede aportar a las empresas grandes cantidades ingentes de información sobre el perfil del individuo que contrata estos servicios. Esta información convenientemente tratada puede arrojar un perfil personal o target específico del individuo que posibilite el envío posterior de publicidad personalizada. Este rastro de información unido a la personalización de la navegación de la telefonía de tercera generación (siempre llevamos el teléfono móvil con nosotros) puede constituir una nueva forma de marketing y publicidad hasta entonces desconocida con grandes beneficios para el sector, siempre y cuando se cumplan los preceptos normativos establecidos en la Ley Orgánica de Protección de Datos de Carácter Personal (en adelante LOPD)."[273]

Más aún, el peligro contra nuestra intimidad puede verse acrecentado si consideramos que a través de un sistema georeferenciado, es perfectamente posible identificar nuestra ubicación exacta mientras llegue señal a nuestro teléfono, y de seguro en poco tiempo la cobertura de la telefonía celular va a ser total. Esto quiere decir que, indirectamente, por medio de la contratación de un servicio de telecomunicaciones, estamos logrando que a través de él se nos pueda seguir perfectamente el rastro.

De ello se desprende que, a medida que la telefonía celular avanza, será necesario adaptarla en Chile a través una debida protección jurídica frente a la protección de datos de carácter personal, y las debidas garantías que el ordenamiento jurídico chileno ofrece para proteger la vida privada de las personas.

Otras Nuevas Tecnologías:

Junto con un avance en el ámbito computacional y comunicacional, Internet se irá ampliando a otras cosas de uso cotidiano. Sin pretender tener una visión extremadamente futurista ni menos caer en ciencia ficción, se pueden hacer los siguientes alcances.

En el campo automotriz, existen desde hace algún tiempo computadores incluidos en los automóviles. Estos sistemas computacionales, como muchos otros, se han ido perfeccionando con el pasar de los años. Dentro de este proceso, se ha incluido ya Internet junto con otras tecnologías. Entre ellas está el sistema de navegación, que permite a los conductores, a través de comunicación satelital, determinar vías alternativas para llegar a un punto o conocer el tráfico en ciertas partes. Conocer la mejor alternativa para ir a un centro comercial, o un parque nacional, etc... Además, se puede recibir publicidad, ver las noticias, entre otras cosas. De ello se puede concluir que, sin mayor dificultad, a través de un sistema satelital se puede determinar a donde nos

[273] Fernando RAMOS SUÁREZ, ESPAÑA: Implicaciones jurídicas de la tecnología UMTS, pág 3 de texto publicado en http://vlex.com/redi/No._30_-_Enero_del_2001/2, visitado en enero del 2002.

dirigimos, con que frecuencia y con que intenciones; y ello, claro está, atenta contra la vida íntima de las personas.

Quienes poseen en la actualidad agendas electrónicas también están al tanto que su capacidad es cada vez mayor no solo en cuanto a la memoria o la velocidad para almacenar información, sino que para conectarse a un computador e incluso para navegar por Internet. Eso también pone en riesgo que en poco tiempo las agendas personales dejen, en todo caso, de ser tan personales.

Otros aparatos como los refrigeradores también comienzan a desarrollar tecnologías que les permitan, a modo de ejemplo, poseer una conexión hacia un computador que de cuenta de las cosas que éste necesita, o que éste va a requerir. [274]

Ejemplos como estos hay muchos, y en poco tiempo más se van a multiplicar. Por ello, con la llegada de la "Sociedad de la Información", es probable que igualmente se comiencen a revelar de cada uno de nosotros un perfil que a lo mejor queremos que no se de a conocer, porque legítimamente lo consideramos personal o íntimo. Ello puede traer consecuencias fatales por ejemplo a la hora de querer contratar un seguro de vida, solicitar un crédito al banco, invertir en un negocio, buscar educación para nuestros hijos, irnos de vacaciones, y cuantas cosas más.

A continuación, se analizarán en el próximo capítulo diferentes prácticas que se llevan a cabo en la actualidad con mucha frecuencia en Internet y que constituyen verdaderas amenazas contra el derecho a la vida privada de las personas.

[274] Un buen sitio web para conocer los alcances de la tecnología que aparecen día a día es el de www.notiac.com, donde se describe el funcionamiento de las últimas versiones de teléfonos celulares, agendas electrónicas, computadores, etc...

CAPÍTULO V: DE LAS DISTINTAS MANERAS DE ATENTAR CONTRA LA VIDA PRIVADA DE LAS PERSONAS A TRAVÉS DE INTERNET

Mark Grant, destacado jurista norteamericano y catedrático de la Universidad de Stanford, California, no se equivocaba al argumentar en su obra Law of the Internet que "*la historia de la tecnología es también la historia de la invasión de la vida privada*"[275]. Y es que efectivamente, con la llegada de nuevos medios de comunicación como Internet, las posibilidades de conocer datos que consideramos personales y de que ellos sean conocidos sin nuestro consentimiento se han multiplicado. Aparte de ser la red una nueva alternativa para violar nuestro derecho a la vida íntima, también es una herramienta que permite facilitar métodos tradicionales para hacerlo.

Profundizando en este punto, el español Antonio Pérez Luño señalaba que: "En etapas anteriores el respeto a la vida privada podía realizarse mediante el uso de los sentidos tales como la vista y el oído. Se permanecía así dentro de los límites de las relaciones naturales. Los muros de una casa, la soledad de un lugar desierto, incluso el tono expresivo oral de un susurro, eran suficientes para asegurar la protección de la intimidad y para excluir el conocimiento y la difusión de las acciones y de las palabras de un individuo o de varias personas unidas entre sí por el vínculo de la confidencia. Hoy es posible observar y escuchar a distancia, sin límites de tiempo, de espacio o de modo; se pueden realizar fotografías en la noche, establecer comunicación simultánea de imagen y sonido con distintos lugares gracias a los circuitos televisivos, dejar involuntariamente el testimonio registrado de la propia imagen o de las conversaciones mantenidas e, incluso, se pueden confesar los propios pensamientos sin el uso de la tortura física y casi inadvertidamente".[276] De hecho, nadie puede tener certeza de la identidad de la persona o institución que está al otro lado del computador cuando navegamos por la red, y menos conocer sus intenciones.

Por ello, a continuación trataré de hacer una reflexión jurídica, acompañada de una breve descripción tecnológica acerca de los medios que la red ofrece para que se obtengan datos o informaciones propios de la vida privada de las personas. Sin embargo, los casos que se expondrán a continuación no tienen el carácter de taxativos, pero sí son las principales amenazas de nuestro objeto de estudio.

1.- La violación al correo electrónico:

Dentro de la esfera que comprende la vida privada de las personas, la correspondencia ha sido uno de sus principales componentes, y su inviolabilidad tiene reconocimiento constitucional en muchos

[275] Mark LEMLEY, Law of the Internet, pág. 111.

[276] Citado por Amílcar MENDOZA LUNA en Perú: Los cookies ¿amenaza a la privacidad de información en la internet?, pág. 2 de texto publicado en http://vlex.com/redi/No._30_-_Enero_del_2001/8, visitado en enero del 2002.

ordenamientos jurídicos, como en el chileno. Con la llegada de Internet, una nueva alternativa de correspondencia se ha popularizado alrededor del planeta: el llamado correo electrónico, o e-mail (electronic mail).

Fue inventado en 1972 por Ray Tomlinson, un experto científico en informática que trabajaba para la consultora de ingeniería estadounidense Bolt, Beranek & Newman, que creó un sistema bastante simple por el cual se podía enviar un mensaje de un computador a otro.[277] Pero su uso masivo se disparó con la popularización de los servicios de Internet. En la actualidad se puede afirmar, sin temor a equivocarse, que el uso de la correspondencia digital es uno de los principales motivos a la hora de utilizar la red. Se dice que durante el año 2001, sólo en Estados Unidos más de 135 millones de personas tendrían una cuenta de correo electrónico, y se calcula que circulan diariamente por la red cerca de 500 millones de mensajes enviados (sólo en Norteamérica).[278] Según un reportaje de fecha 10 de diciembre de 2001 del diario El Clarín argentino, circularían cerca de 9.800 millones de e-mails al día, y de seguro esta cifra aumenta cada día.

Muchos han confundido al correo electrónico con el correo tradicional, pretendiendo de esta manera aplicar las mismas normas y los mismos principios entre uno y otro. La verdad es que eso es un error, ya que existen esenciales diferencias que hacen que el e-mail sea un medio de comunicación con características totalmente particulares.

Cuando uno utiliza el correo tradicional, puede servirse de distintos métodos para darle mayor o menor seguridad a la carta o mensaje que se envía. Si se trata por ejemplo de una postal, uno descuida que se lea lo que ella contiene sabiendo que de por sí no tiene ninguna seguridad que la resguarde. Pero, si se trata de un mensaje que requiere mayor cuidado en cuanto a su contenido, se puede optar por enviarlo a través de un sobre sellado, por carta certificada, por un servicio de correo especial o más caro, por exigir una entrega personal del mismo, etc... Tratándose de mensajes enviados a través del correo electrónico, no existe garantía

---

[277] El 10 de diciembre de 2001, el diario argentino El Clarín publicó un artículo titulado "CADA DÍA CIRCULAN 9.800 MILLONES DE E-MAILS El correo electrónico cumple 30 años". He querido reproducir un extracto de esta noticia para ilustrar un poco la historia de este medio de comunicación: "Si bien era muy conocido por sus programas, Tomlinson se hizo mucho más famoso por una simple decisión que tomó al programarlo: necesitaba una manera de separar el nombre del usuario del nombre de la máquina en la que estaba ese usuario y, por casualidad, depositó la vista en el símbolo @, que terminó convirtiéndose, sin que él se diera cuenta, en un ícono del mundo conectado.(...) En los 70, enviar un e-mail era sencillo, pero intentar leerlo o responderlo era un gran problema, ya que aparecían pegados y no existía la función "Respuesta". Lawrence Roberts, que por entonces era gerente de la oficina de Técnicas de Procesamiento de Información de la Advanced Research Projects Agency, se abocó a resolver el problema cuando su jefe empezó a quejarse del volumen de e-mails que se apilaba en su bandeja de entrada. En1972, Roberts produjo el primer administrador de e-mails, llamado "RD", que incluía un sistema de archivo y una función "Borrar". Otras mejoras posteriores llegaron de la mano de John Vittal, que en los años 70 era un joven programador del Institut o de Ciencias de la Información de la Universidad de Southern California, EE.UU.. Vittal pasó muchas horas trabajando en el programa, al que llamó MSG. Y no sólo incluyó el comando "Borrar", sino, también, la función "Responder". Cada vez más, la funcionalidad del e-mail adquirió las características de la correspondencia convencional. Vittal también sumó las funciones "cc" y "bcc"."

[278] Edward GOOD, An e-mail Education. What You D'ont Know About E-Mail Can and Will Hurt You, citado por María Helena Barrera en Correspondencia Digital: Recreando Privacidad en el Ciberespacio, pág 12 de texto publicado en http://www.digital-law.net/IJCLP/3_1999/ijclp_webdoc_4_3_1999.html de International Journal of Communications Law and Policy, Summer 1999, Oxford University, visitado en enero del 2002.

alguna sobre la no violación de la correspondencia digital, ya que como se verá más adelante, antes que el mensaje llegue a su destino, pasa por distintas etapas en las cuales fácilmente puede revelarse su contenido.

Un correo electrónico puede duplicarse en forma infinita, ya que un mismo mensaje puede por ejemplo mandarse a uno o a varios destinatarios, todo ello en segundos, con la misma calidad y sin costo. Si a través del correo tradicional se quiere mandar un mensaje a varias personas, es necesario reproducirlo materialmente, y realizar la operación por separado para cada destinatario. Ello toma mucho tiempo y dinero. Además, no existe garantía alguna respecto de las condiciones en que se va a recibir dicho mensaje.

El e-mail es ubicuo, ya que no tiene un destino físicamente determinado, sino que puede ser recogido a través de cualquier computador que se encuentre conectado a Internet en cualquier parte del mundo. El correo tradicional por su parte requiere de una casilla postal o de una dirección perfectamente determinada para llegar a su destino final.

El correo electrónico funciona a través de una página web[279] que provee de este servicio a los usuarios, independientemente donde éstos se encuentren. Está página de acceso permite que el titula de la cuenta ingrese a su correo mediante la combinación de dos elementos: el nombre del usuario (en inglés *login*) y su contraseña (en inglés *password*). Según Geraldo Quintero, "el primero siempre se expresa en el idioma, código o signo identificable y legible; y el segundo se registra en caracteres ilegibles e identificables y es la llave personal con la que cuenta el usuario para impedir que terceros puedan identificarla y acceder a ella".[280] Incluso, la propia página de acceso a la cuenta de correo electrónico ofrece servicios en caso de que la clave de acceso haya sido olvidada. El correo tradicional funciona a través de un servicio postal bastante distinto.

Hechas las distinciones pertinentes, podemos a entrar a definir al correo electrónico, e-mail o *electronic mail* como la "aplicación mediante la cual un ordenador puede intercambiar mensajes con otros usuarios de

---

[279] Una dirección de correo electrónico está compuesta de un identificador de usuario y de un identificador del ordenador, unidos por el carácter @. Ejemplo: fcoronel@puc.cl, y en este caso el servidor sería la Pontificia Universidad Católica (puc), situada en Chile (cuyo identificador de país o subdominio se conoce como cl).Existen tres tipos de cuenta de correo: 1) Cuenta gratuita: Nuestro servidor de correo nos permite personalizar el nombre del usuario (siempre que en este servidor no exista otro usuario con el mismo nombre, en cuyo caso debemos elegir otro). Ejemplo: fcoronel@hotmail.com, el grado de personalización por lo tanto es nulo, este es un tipo de cuenta destinada a usuarios finales. 2) Cuenta con subdominio: En este caso nuestro servidor además de nombre de usuario nos permite incluir un subdominio propio, aunque siempre aparezca vinculado al dominio de nuestro servidor. Ejemplo: felipe@coronel.hotmail.com y 3) Cuenta con nuestro propio dominio: Al tratarse del dominio propio el grado de personalización es completo puesto que no se identifica con ningún servidor ajeno a la empresa. Ejemplo: felipe@coronel.com Los servidores se pueden identificar por uno o dos nombres, más el nombre de la organización (puc) y el identificador del país (cl). Información obtenida a través de http://www.baluma.com/internet1al10/servicios.asp, visitada en marzo de 2002.

[280] Argido GERALDO QUINTERO, Colombia: El Secreto en la Comunicación por Correo Electrónico, pág. 3 de texto publicado en http://publicaciones.derecho.org/redi/No._25_-_Agosto_del_2000/3, visitado en enero de 2002.

ordenadores (o grupos de usuarios) a través de la red. El correo electrónico es uno de los usos más populares de Internet. Dícese también de los mensajes enviados a través de este medio."[281]

De lo anteriormente explicado se pueden también determinar las características del correo electrónico[282]:

1.- Virtual: representa una nueva forma de comunicarse entre las personas a través de un espacio no físico.
2.- Múltiple: ya que pueden existir infinidad de copias de un mismo mensaje.
3.- Ubicuo: puede encontrarse en cualquier parte del mundo donde exista un ordenador conectado a la red.
4.- Instantáneo: puede estar en segundos en su lugar de destinos y además todos los computadores que estén interconectados a través de Internet.
5.- Reproducible: porque puede crearse un número infinito de sus copias
6.- Manipulable: porque la naturaleza misma del correo electrónico obliga al operador del sistema a manipular y enrutar mensajes.

La cuenta de correo electrónico, desde mi punto de vista, debe ser considerada como un dato de carácter personal, y por consiguiente, debe resguardársele con todas las garantías que la Ley 19.628 ofrece a los datos considerados tales. Esta protección ya ha sido reconocida, como lo señala Paloma Llaneza González, por el Consejo Europeo, que derechamente afirma que "la dirección de correo electrónico es un dato personal".[283] Esto confirma que la cuenta de correo electrónico y su contenido forman parte de la esfera íntima de las personas, y por consiguiente merece la protección que se le ha reconocido.

La intercepción de correos electrónicos es bastante más común de lo que los usuarios se imaginan. Ello se debe en gran medida al funcionamiento del sistema, que en muchos casos obliga a quienes lo prestan a cometer este ilícito procurando que no pase como tal. Entidades que prestan el servicio de correo electrónico como Hotmail o Yahoo![284] reconocen que debe existir secreto en cuanto al contenido y uso que cada persona

[281] Definición obtenida de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[282] Para ver con más detalle estos puntos, remitirse a Argido GERALDO QUINTERO, Colombia: El Secreto en la Comunicación por Correo Electrónico, de texto publicado en http://publicaciones.derecho.org/redi/No._25_-_Agosto_del_2000/3, visitado en enero de 2002.

[283] Paloma LLANEZA GONZÁLEZ, Internet y Comunicaciones Digitales, pág. 271, Editorial Bosch, Barcelona, España, 2000.

[284]Según lo señala el colombiano Argiro GERARLDO QUINTERO, "Hotmail empresa del potentado Microsoft consagra el secreto a la comunicación por correo electrónico así. " Es política de Microsoft respetar la privacidad de sus usuarios. Microsoft no supervisará, modificará o divulgará ninguna información de carácter personal acerca de usted o del uso que usted haga del Servicio. Incluidos sus contenidos, sin su previo consentimiento, a menos que Microsoft considere de buena fe que dicha actuación es necesaria para 1)cumplir con requerimientos o procedimientos legales,2) proteger y defender los derechos o propiedad de Microsoft,3) hacer cumplir las CDS ,o 4) actuar para proteger los intereses de sus usuarios o terceros ...". Yahoo! igualmente expresa una política de privacidad así: "el usuario reconoce y acepta que Yahoo! no examinará lo contenidos con anterioridad a su puesta en disposición o trasmisión, pero éste y sus representantes estarán facultados (ero no obligados) a rechazar o desplazar cualquier contenido que esté disponible en el Servicio. Sin perjuicio de lo anterior , Yahoo! y sus representantes estarán plenamente facultados para suprimir cualquier

haga de su cuenta de correspondencia digital. Así mismo, cuando los usuarios contratan este servicio, se someten a un contrato de adhesión en el cual se determina como territorio jurisdiccional aquel en el cual se encuentra establecida la dirección comercial de la página web. Estos proveedores del servicio de correo electrónico generalmente justifican una intervención en la cuenta de los usuarios cuando se trata de cumplir con procedimientos legales o velar por el adecuado funcionamiento del sistema. Las palabras del norteamericano Barry Fraser ilustran esto de la siguiente manera: "Su mensaje electrónico puede ser manejado por muchos servicios digitales durante su envío. El operador de sistema de cada uno de esos sistemas puede ver el contenido del mensaje bajo alguna de las excepciones consagradas en el ECPA. Adicionalmente, el mensaje puede ser interceptado si el remitente o el destinatario del mensaje consiente. En consecuencia, incluso si usted no ha consentido a tal intercepción o acceso, la persona a quien se envió el mensaje puede haber consentido a tales actividades."[285] Profundizando en las consecuencias de lo que esto puede traer, muchos han puesto en tela de duda las políticas que estos servidores ofrecen a sus usuarios, ya que muchas veces los intereses económicos pueden más que la protección de intereses legítimos.[286]

Aparte de esto, la correspondencia digital también se ve amenazada por los llamados *hackers*, quienes a su vez buscan destruir los sistemas de seguridad que los proveedores del servicio tienen, para de esta manera poder acceder a las cuentas de correo de sus miembros. Esta práctica también es muy común alrededor del ciberespacio, y su control no ha dado los suficientes frutos.[287]

Esto no se limita a lo anteriormente expuesto, ya que existen también quienes se han dedicado a utilizar correos electrónicos de otros como propios. Un caso curioso y sonado es el que sucedió con fecha 2 de abril

---

Contenido que vulnere las Condiciones o que de algún modo sea inaceptable...."." Colombia: El Secreto en la Comunicación por Correo Electrónico, de texto publicado en http://publicaciones.derecho.org/redi/No._25_-_Agosto_del_2000/3, visitado en enero de 2002.

[285] Barry FRASER, Rules of the road navigating the information superhigway, 26 WTR Hum. Rts 17,18, citado por Maria Helena BARRERA en Correspondencia Digital: recreando privacidad en el ciberespacio, pág. 11 de texto publicado en en http://www.digital-law.net/IJCLP/3_1999/ijclp_webdoc_4_3_1999.html de International Journal of Communications Law and Policy, Summer 1999, Oxford University, visitado en enero del 2002.

[286] A este respecto, Jeremy POMEROY, en Online anonymity can be illusory under current law, ISP policies (4 No. 12 MMEDIAST 1) señalaba que "En cualquier caso, la protección ofrecida por los proveedores de Internet mediante sus "Políticas de privacidad", es típicamente sujeta a cambios. Los proveedores se reservan tradicionalmente el derecho de revisar y transformar los términos de dichas políticas sin previo aviso a los usuarios. En consecuencia, un usuario que confíe en un determinado nivel de protección conferido de acuerdo a una política de privacidad determinada, puede encontrarse de repente con que los detalles íntimos que, voluntaria o involuntariamente reveló a su proveedor, han sido puestos a disposición de terceras partes." citado por Maria Helena BARRERA en Correspondencia Digital: Recreando Privacidad en el Ciberespacio, pág 13 de texto publicado en http://www.digital-law.net/IJCLP/3_1999/ijclp_webdoc_4_3_1999.html de International Journal of Communications Law and Policy, Summer 1999, Oxford University, visitado en enero del 2002.

[287] "El 24 de agosto de 1999 un cambio en la configuración del sistema dejó vulnerables los buzones de la totalidad de usuarios. Hackers descubrieron la falla, crearon un programa que permitía libre acceso a cuentas Hotmail y lo pusieron en libre uso en el Internet. Hasta el 30 de agosto, fecha en que el problema en el sistema fue corregido el único control posible fue la obstrucción de sitios que en todo el mundo aparecían con el script que permitía el acceso no autorizado. Localizar y bloquear dichos sitios fue tarea similar a la destrucción de Medusa: Por cada uno neutralizado, algunos otros aparecen de inmediato". Maria Helena BARRERA en Correspondencia Digital: Recreando Privacidad en el Ciberespacio, pág 3 de texto publicado en http://www.digital-law.net/IJCLP/3_1999/ijclp_webdoc_4_3_1999.html de International Journal of Communications Law and Policy, Summer 1999, Oxford University, visitado en enero del 2002.

del 2002 en Francia. Allí la prensa manifestaba que: "El Partido Socialista francés interpuso los pasados días una denuncia por la supuesta invitación, mediante correo electrónico, en el nombre de dicho partido a la presentación del programa de Lionel Jospin el próximo jueves en París. Según parece el correo desde el cual se dirigía el texto fue enviado desde la dirección electrónica @parti-socialiste.fr."[288].

Estamos concientes de que el uso de correos electrónicos personales por terceros es también una práctica muy común y de la que seguramente a lo mejor los afectados nunca se llegan a enterar. Por supuesto que las consecuencias de ello también afectan la vida privada de los dueños de las casillas electrónicas.

Muchas propuestas en torno a cómo afrontar este problema han surgido por todo el mundo y de todos los tipo. Hay quienes ven una solución en la creación de un "organismo multinacional"[289], otros creen que la solución está en manos de los proveedores del servicio de Internet, más precisamente los operadores del sistema a cargo de su manejo. Están los que creen que la solución es crear un sistema que torne imposible la identificación de la persona que envía los mensajes, con la obvia excepción del destinatario.[290]

Otros, como la ecuatoriana Maria Helena Barrera, creen que en la creación de un sistema de seguridad criptográfico está la solución más viable. Comparto esta postura, aunque sin embargo, al ser el correo electrónico uno de las posibilidades de correspondencia más usadas del mundo, la existencia de una solución que combine armoniosamente aspectos técnicos y jurídicos se vuelve relevante, sobre todo en un mundo en que ya todos admiten que el ciberespacio no ofrece ninguna garantía segura y confiable en el ámbito de la correspondencia digital.

2.- El Correo No Deseado:

Antes de la llegada de Internet, el uso del teléfono y del fax en oficinas y lugares comerciales era vital a la hora de comunicarse con los demás. Durante los años en que este medio de comunicación tuvo su

[288] Información obtenida en http://delitosinformaticos.com/noticias/101761230840490.shtml, visitado en abril del 2002.

[289] Argino GERALDO QUINTERO ha dicho que "La creación de un organismo multinacional, llámese gobierno ciber o organización internacional de regulación cibernética es necesaria para garantizar a todos los ciudadanos del mundo el secreto de sus comunicaciones por la red y los derechos a la intimidada, El desarrollo incalculable del servicio de Internet va unido el del correo electrónico, en 1999 solo Hotmail tenía 40 millones de usuarios, es pues urgente llamar la atención sobre unas regulaciones globales que permitan eficazmente garantizar los derechos fundamentales del hombre la tecnología y el temor de los estados a ser vulnerables por la criminalidad globalizada no pude acabar con las conquistas humanas en materia de derechos fundamentales." Colombia: El Secreto en la Comunicación por Correo Electrónico, pág. 12 de texto publicado en http://publicaciones.derecho.org/redi/No._25_-_Agosto_del_2000/3, visitado en enero de 2002.

[290] María Helena BARRERA se refiere a los inconvenientes de esta solución en el sentido de que: "Los problemas que conlleva esta solución son duales: En primer lugar anonimidad no puede ser sinónimo de privacidad, desde un punto de vista legal. Anonimidad es solo una de las posibilidades que la privacidad brinda, uno de los componentes de un derecho mucho mas vasto y global. En segundo lugar, anonimidad puede ser destruida en cualquier momento, por regeneración legítima o ilegítima de la traza que conecta (incluso en los mejores instrumentos), el mensaje con su creador." Correspondencia Digital: Recreando Privacidad en el Ciberespacio, pág 8 de texto publicado en http://www.digital-law.net/IJCLP/3_1999/ijclp_webdoc_4_3_1999.html de International Journal of Communications Law and Policy, Summer 1999, Oxford University, visitado en enero del 2002.

auge, surgieron quienes se dedicaban a enviar diariamente publicidad a través del fax, o quienes a través de grabadoras llamaban por teléfono promocionando algún producto. Esto seguramente le hizo pasar más de un mal rato a quien, por causa de esta publicidad no deseada, perdía tinta de su fax, tiempo y dinero. En países como Estados Unidos, este problema fue combatido a través de la dictación de normas como la TCPA o *Telephone Consumer Protection Act* de 1991, que regularía la llamada publicidad no deseada a través del fax y del teléfono. [291]

Con el desarrollo y uso masivo del correo electrónico en el mundo, muchos también vieron en esta manera de comunicarse con las personas una excelente vía a la hora de hacer publicidad. De esta manera, es común entre quienes tienen una cuenta de correo electrónico recibir con muchísima frecuencia correos no solicitados o "mensajes basura".

Se ha clasificado al correo electrónico no deseado en *Spam* o *Junk Mail* según si tiene o no intenciones comerciales. Es así que se define al *Junk Mail o Garbage Mail* como el "correo basura que, por lo general, no tiene carácter comercial y que suele provenir de direcciones no anónimas. Los casos más frecuentes son las pesadísimas cartas cadenas ("chain letter) sobre la buena o mala suerte, virus informáticos inexistentes, niños gravemente enfermos que desean recibir correos electrónicos de todos los confines de la tierra."[292] Desde un punto de vista más general, otros lo han definido de la siguiente manera: "Dícese de la propaganda indiscriminada y masiva llevada a cabo a través del correo electrónico. Es una de las peores plagas de Internet y concita un amplio rechazo hacia quien lo practica"[293].

El llamado *Spam, Bombardeo Publicitario o Buzonfia* se define tradicionalmente como el "Envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico. Literalmente quiere decir loncha de mortadela".[294] Se trataría en este caso de publicidad que tiene intenciones comerciales. Se cree que cerca del 30% de los mensajes que se mandan a través de Internet constituyen correos electrónicos no deseados. [295]

La doctrina ha considerado que el correo electrónico no deseado produce dos efectos: el primero es que se incurre en un gran costo que tiene que ser afrontado tanto por el dueño de la cuenta de correo como por quien

---

[291] Ver más sobre este tema en texto de Carlos Alfredo LEÓN LEÓN en Perú: Consideraciones Legales Relativas al Envío de E.mails Comerciales No Solicitados, pág. 4 de texto publicado en http://vlex.com/redi/No._36_-_Julio_del_2001/13, visitado en enero de 2002.

[292] Paloma LLANEZA GONZÁLEZ, Internet y Comunicaciones Digitales, pág. 271, Editorial Bosch, Barcelona, España, 2000.

[293] Definición obtenida de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[294] Ibídem.

[295] Esta cifra, según Carlos Alfredo LEON LEON en Perú: Consideraciones Legales Relativas al Envío de E.mails Comerciales No Solicitados, corresponde a un estudio efectuado por America On Line (AOL), de un total de 30 millones de mails que circulan a través de este servidor diariamente. Esta información se puede encontrar en pág. 2 de texto publicado en http://vlex.com/redi/No._36_-_Julio_del_2001/13, visitado en enero de 2002.

provee de acceso a Internet; y el segundo es que se trata de una manera más de atentar contra la esfera privada de las personas a través de este medio.

Se dice que la Comisión Europea ha calculado que unos 500 millones de "spams" se envían diariamente, y que ello representa una pérdida mundial de cerca de 9.300 millones de dólares al año. [296] Esto se traduciría por ejemplo en el tiempo en que uno se demora en leer y eliminar estos correos. Desde otra perspectiva, muchos páginas web que prestan el servicio de correo electrónico permiten que nuestras casillas ocupen una cierta cantidad de espacio. Por consiguiente, si nos vemos bombardeados de estos mensajes no deseados, se borrarán otras comunicaciones que sí pueden ser importantes para el usuario. Todo ello, a la larga trae pérdidas calculables en dinero, generando responsabilidades extracontractuales.

Pero el tema que realmente nos interesa es el enfoque que debe dársele a este correo como atentatorio de nuestro derecho a la vida privada. Como se señalaba anteriormente, la casilla de correo forma parte de nuestra esfera íntima, y por consiguiente el acceso a ella y el uso que los demás pretendan otorgarle no tiene el carácter de libre y debe respetarse. A más del hecho de que los usuarios que tienen casilla electrónica se ven abrumados alevosamente de información que no ha sido solicitada, debe considerarse que la información de su dirección de correo electrónico, que es un dato personal, ha sido revelada sin su consentimiento.

En efecto, generalmente los correos no solicitados son enviados a una serie de personas al mismo tiempo, y ello responde al hecho de que ,detrás de estos mensajes, existe una base de datos que contiene información de cada una de las personas que reciben esta correspondencia. Es casi seguro que aquella base de datos no cumpla con los requisitos que establecen normas como la Ley 19.628 del ordenamiento jurídico chileno, y por consiguiente se trate de bases de datos ilegales, obtenidas a través de métodos ilícitos y utilizadas para fines contrarios a la ley. De todo ello se desprende que los correos no solicitados son ilegales y atentan contra nuestro derecho a no ser molestados, a que se respete aquella parte de nuestras vidas considerada como íntima.

En los Estados Unidos, este problema ya ha tenido que ser afrontado por los tribunales. Como lo señala Waldo Augusto Roberto Sobrino, "Entre las primeras Sentencias referentes a la cuestión del "spam", es menester recordar "Cyber Promotions Inc. vs. America Online Inc." y "America Online Inc. vs. Cyber Promotions Inc.", tramitada en la Corte de Pennsylvania, de fecha 4 de Noviembre de 1996, donde entre varias interesantes cuestiones, la empresa acusada de "spam", basaba su defensa en la "Primera Enmienda" ("free speech rights"), e -incluso- se analizó la legalidad de "America Online" de enviar "e-mail bombs"".[297]

---

[296] Citado por Waldo Augusto ROBERTO SOBRINO en Argentina: Las "Cookies" y el "Spam" (y la violación de la "Privacidad" y la "Intimidad"). Un análisis desde la óptica del derecho argentino, pag. 7 de texto publicado en http://vlex.com/redi/No. 35 - Junio del 2001/3, visitado en enero de 2002. Esta información se habría obtenido en www.baquia.com , de fecha 2 de mayo de 2001.

[297] Ibídem, pág13, refiriéndose a información obtenida en Electronic Comerse & Law Report, de fecha 1 de Diciembre de 1997, publicado en http://zeus.bna.com/e-law/cases/aolcyb2.html .

Como consecuencia de ello, existen ya en el Congreso Norteamericano un proyecto de ley, la *Unsolicited Electronic Mail Act* del 2000 (H.R. 3113), actualmente en discusión por el Senado de ese país. Se dice que "Este proyecto establece que el e-mail comercial no solicitado se encuentre marcado o rotulado como tal y que se incluyan en el mismo procedimientos para solicitar el retiro de las listas de distribución. Prohíbe asimismo que estos mensajes sean enviados utilizando las facilidades de proveedores (ISP) que hayan señalado expresamente que la prohibición de enviar estos mail utilizando sus servicios".[298] Sin embargo, la dictación de cualquier norma referente a Internet debe considerar el problema de la a-territorialidad de la red, ya que como veíamos anteriormente, la aplicación de una ley tiene cabida en un territorio jurisdiccional determinado, y en Internet el espacio físico no existe.

Muchos vieron una solución a través de los sistemas *Opt-in* y *Opt-out*. Mediante el primero, se establece que quien desee recibir algún tipo de correo electrónico no solicitado debe manifestarlo a través de su inscripción en una lista, vale decir, tiene que prestar su consentimiento para ello. El segundo sistema por su parte establece que es legítimo enviar este tipo de mensajes, salvo que el destinatario de éstos manifieste lo contrario. Dentro de estas dos posibilidades, el sistema *Opt-in* ha tenido mayor aceptación tanto en Estados Unidos (que lo adoptó en la *Telephone Consumer Protection Act*) como en Europa[299]. Obviamente que los partidarios del otro sistema, como las empresas de marketing, defenderán su derecho a hacer publicidad por este medio.

Otra solución presentada por los expertos en el sistema es la inclusión de filtros en los servidores, por medio de los cuales se detectaría y se imposibilitaría el ingreso de correos no solicitados. Se pretende que por medio de estos filtros, se detecte a estos mensajes que son enviados a través de ciertas palabras o expresiones, o de alguna dirección identificable. Sin embrago, aún cuando la solución puede ser buena, se debe considerar la posibilidad de que quienes envían esta correspondencia tratarán de "disfrazar" estos mensajes, de tal manera que no sean detectados por estos filtros y puedan llegar a su destino.

---

[298] Citado por Carlos Alfredo LEÓN LEÓN,Perú: Consideraciones Legales Relativas al Envío de E.mails Comerciales No Solicitados, pág. 4 de texto publicado en http://vlex.com/redi/No._36_-_Julio_del_2001/13, visitado en enero de 2002.

[299] Con fecha 7 de diciembre de 2001, se publicó la siguiente noticia, de gran interés en lo que concierne al Spam y a las Cookies (que serán tratadas más adelante) y que señala que: "El Consejo de Ministros de Telecomunicaciones de la UE ha aprobado la propuesta de Directiva sobre regulación del correo comercial no deseado (spam), optando por la opción 'opt-in' que obligará a las empresas a obtener la autorización previa expresa del internauta para poder enviarle este tipo de correos electrónicos. La reunión de los encargados en materia deTelecomunicaciones en los Quince sirvió, además depara la presentación por la Comisión del Séptimo Informe sobre la Implementación del Paquete Legislativo sobre Telecomunicaciones, para la adopción por parte de los representantes de los estados miembros de la propuesta de Directiva de la Comisión sobre regulación del denominado 'spam'. Finalmente, los Quince han optado por la opción 'opt-in' por la que las empresas que deseen remitir correos comerciales a internautas deberán contar con el consentimiento expreso previo de los destinatarios, con la excepción de que ya exista una relación contractual comercial entre ambas partes. Los ministros europeos también han aprobado el refuerzo de la protección del ciudadano en la Red atravéss de la introducción de ciertas condiciones para el uso de las denominadas 'cookies', de forma que los internautas tengan la opción de rechazar el uso de las mismas en sus conexiones a la Red. Las medidas aprobadas en la reunión de ayer en Bruselas deberán ser sometidas ahora al Pleno del Parlamento Europeo, donde se espera que la propuesta de Directiva sobre 'spam' cuente con el rechazo de la mayoría de la Cámara." Esta noticia se obtuvo de la página http://v2.vlex.com/es/asp/noticias_detalle.asp?Articulo=118803, visitada en abril de 2002.

Hay quienes creen que la autorregulación todavía puede ser una alternativa, pero son los que menos, ya que está demostrado que en un mundo donde los intereses valen más que la buena fe, este tipo de soluciones se vuelven un tanto utópicas.

3.- Las *Cookies* o Galletitas:

Se definen tradicionalmente como *cookie* (espía, cookie, *cuqui* ,fisgón, galletita) al "conjunto de caracteres que se almacenan en el disco duro o en la memoria temporal del ordenador de un usuario cuando accede a las páginas de determinados sitios web. Se utilizan para que el servidor accedido pueda conocer las preferencias del usuario al volver éste a conectarse. Dado que pueden ser un peligro para la intimidad de los usuarios, éstos deben saber que los navegadores permiten desactivar los (¿o las?) cuquis". [300] Otros han preferido definirlas como "ficheros de datos guardados en un directorio específico del ordenador del usuario. Se crean por los sevidores web con el objeto de ser envíados a los programas navegadores del usuario, y así recoger la información que dicho fichero ha reunido". [301]

Se clasifican en:

- Cookies persistentes: se almacenan como un archivo en el equipo y permanece en él cuando se cierra el servicio del navegador.
- Cookies temporales o de sesión: son aquellas que se almacenan únicamente durante la sesión de navegación actual y se eliminan al terminarse el uso del servicio del navegador
- Cookies de primeros frente a cookies de terceros: una cookie de primero es aquella que se origina en el mismo sitio web que se visita ese momento, o bien se envía a éste y se utiliza para almacenar información. Una cookie de tercero se origina en un sitio web diferente al que se visita en ese momento, o se envía a éste. Se utiliza frecuentemente para realizar un seguimiento para conocer el uso que el navegador le da a la página web. Las cookies de tercera pueden a su vez ser persistentes o temporales.
- Cookies inapropiadas: son cookies que pueden permitir el acceso a información de identificación personal que se podría usar para otros fines sin su consentimiento. [302]

Desde un punto de vista técnico, Miguel S. Elías las describe considerando los siguientes puntos:

---

[300] Definición obtenida del Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[301] Fernando RAMOS SUÁREZ, ¿Es legal el uso de Cookies?, pág. 1 de texto publicado en http://vlex.com/redi/No._01_-_Agosto_de_1998/ramos, de página visitada en enero de 2002.

[302] Esta clasificación se encuentra en la descripción que el servicio de navegación de Internet Explorer 6.0 ofrece al usuario al momento de solicitar autorización para instalar una cookie en el computador de los usuarios.

"-Para empezar, lo que se deja en el disco duro del usuario es un inofensivo fichero de texto (con extensión ".txt") y no un fichero ejecutable (".exe", ".com", ".bat", etc.), por lo que no existe posibilidad alguna de que una "cookie" sea en realidad un virus informático.

-Las "cookies" no pueden "ver" ningún dato del disco duro del usuario, ni pueden determinar la dirección de e-mail o la identidad del usuario. Estos datos sólo los puede obtener un sitio Web, si el usuario los facilita de una manera voluntaria.

-Las "cookies" no pueden tener un tamaño desmesurado. De hecho, no pueden sobrepasar los 4 kbs cada una de ellas.

-Un sitio Web sólo puede recoger las "cookies" que dejó él mismo, es decir, no puede recoger las "cookies" provenientes de otros sitios."[303]

Para su aplicación, muchos servidores utilizan el sistema *Opt- in*, es decir que piden el consentimiento del usuario para la instalación de las Cookies. Sin embargo, no siempre esta política ha sido respetada.

Se dice que fue creado por la empresa Netscape en 1995 para uso de la versión 2.0 de su navegador. Tiene como función original el hacer que se recuerde y reconozca a un usuario cada vez que ingrese a una página web. Ello en teoría buscaba también que la navegación por Internet sea más personal y conveniente. En realidad se trata de una información valiosa, producto de las huellas que dejan los usuarios durante su navegación, creando un perfil exacto y minucioso respecto de las preferencias de éstos dentro de la red, sus hábitos de consumo, el tiempo destinado a navegar, sus intereses comerciales, sus posibilidades económicas, etc... Esto es posible ya que cada usuario que visita una página web deja un rastro o número IP (Internet Protocol), que es lo que permite identificar los pasos que éste efectuó mientras navegaba, y las cookies sí pueden tener el número IP del usuario. Por consiguiente, si bien las cookies por sí solas no pueden identificar a quien navega en la red, a través de la lectura de su IP esto se vuelve posible. Puede demostrarse de esta manera su ilegalidad ya que se atenta contra un derecho fundamental de las personas, cual es su vida privada, que se ve desnudada con los datos de carácter personal que este sistema arbitrariamente transmite.

Aún cuando existen mecanismos para desactivar la lectura y escritura de las Cookies, la posibilidad de habilitarlas sin nuestro consentimiento no es tarea difícil.

Esta información de carácter personal constituyen un bien extremadamente cotizado por empresas que se dedican al marketing directo, ya que se trata de bases de datos que revelan las preferencias de los usuarios en la red. Un ejemplo que ilustra perfectamente la amenaza que representa este sistema fue el estudio que hizo la Federal Trade Comisión (FTC) por encargo de Al Gore en 1998. De ello se desprendieron los siguientes resultados: de 1400 websites comerciales visitados, un 85% recogían y almacenaban datos personales de los

[303] Miguel S. ELIAS, Argentina: Situación Legal de los Datos de Carácter Personal frente a las Nuevas Tecnologías, pág. 29 de texo publicado en http://vlex.com/redi/No._32_-_Marzo_del_2001/10, y de página visitada en enero de 2002.

visitantes. Sólo un 14% daban alguna indicación acerca del grado de intimidad de la información recogida y sólo un 2% ofrecía una política a favor de los usuarios con sentido. [304]

En los Estados Unidos existen ya demandas al respecto, y uno de los casos más sonados es el de la empresa *Double Click Company* que tiene como razón social el diseñar estrategias de marketing por Internet a través del estudio del comportamiento de los usuarios mientras navegan. Esta empresa posee cerca de 1.500 sitios de Internet afiliados en todo el mundo, desde los cuales se monitorea a los navegantes. De ello se desprenden, mediante el uso de Cookies, verdaderos perfiles de los usuarios. Se crean así bases de datos obtenidas sin el consentimiento de quienes las forman, y que son muy cotizadas en el mercado. Ello condujo a que en el año 2001, el Centro de Información sobre Privacidad Electrónica denuncie públicamente a esta empresa sobre estas prácticas ilegales. Los demandados se defendieron argumentando que "la promoción es un servicio a todos los consumidores", que "usan las cookies únicamente para asegurar que un usuario no vea el mismo aviso demasiadas veces" y que "esta metodología cuestionada les permite suministrar a sus empresas afiliadas, información precisa para que luego estas sugieran correctamente ciertos productos a los clientes". Este caso ya fue planteado ante la Federal Trade Comisión y en la actualidad se encuentra en la Corte Suprema de los Estados Unidos.[305]

Consideremos el caso de que se vendiera esta información o se analizara de forma incorrecta, ya que podría causar serios problemas. Debido al incalculable alcance de este tipo de empresas y a la difusión que haga de nuestros datos a sus "clientes" se podrían dar hechos inimaginables como el ser rechazados en nuestro trabajo por haber visitado una página web que aboga por la legalización del aborto, o ser vigilados minuciosamente después de hojear información "en línea" acerca de cómo fabricar bombas caseras, o tener que pagar más nuestro seguro después de visitar un sitio con información para pacientes con SIDA.

En la actualidad, hay quienes creen que las Cookies pueden convertirse en un mecanismo que no atente contra el derecho a la vida de las personas a través de un sistema como el del *Opt-in*, y que se ajuste a las exigencias de los ordenamientos jurídicos. Sin embargo, aún cuando exista una aparente buena fe por parte de quienes proponen este sistema, se ha demostrado ya que las llamadas *Galletitas* pueden ser colocadas sin que el usuario se percate, y ello debe considerarse en la actualidad donde la tecnología ha podido más que las buenas intenciones.

---

[304] Información obtenida de David CASCUBERTA, La privacidad en los nuevos medios electrónicos. Aspectos éticos y sociales, pág. 2 de texto publicado en http://vlex.com/redi/No._11_-_Marzo_del_2001/10, visitado en diciembre de 2001.

[305] La información del caso "Double Clic Company" fue obtenida de Miguel S. ELIAS en Argentina: Situación Legal de los Datos de Carácter Personal frente a las Nuevas Tecnologías, pág. 33 de texto publicado en http://vlex.com/redi/No._32_-_Marzo_del_2001/10, de página visitada en enero de 2002. Otro caso conocido es el de *"Judnick vs. DoubleClick"*, de fecha 27 de Enero de 2000, promovido en la Corte de California (Marin City N° CIV 000241) se ha instaurado una acción, peticionando una *"injunction"*, porque la empresa utilizó el sistema "Opt-in", sin el consentimiento expreso del consumidor/usuario. Esta información se encuentra en el texto de Waldo Augusto ROBERTO SOBRINO en Argentina: Las "Cookies" y el "Spam" (y la violación de la "Privacidad" y la "Intimidad"). Un análisis desde la óptica del derecho argentino, pag. 7 de texto publicado en http://vlex.com/redi/No._35_-_Junio_del_2001/3, visitado en enero de 2002.

4.- El derecho a la vida privada y los Proveedores del Servicio de Internet (o ISP):

Cada vez que nos conectamos a la red, requerimos de un servicio, cual es aquel que nos permite conectarnos al ciberespacio. Este servicio lo prestan los llamados *Internet Service Providers* (ISP) o *Proveedores del Servicio de Internet* (PSI). Tradicionalmente se los ha definido como la "Organización, habitualmente con ánimo de lucro, que además de dar acceso a Internet a personas físicas y/o jurídicas, les ofrece una serie de servicios (por ejemplo, hospedaje de páginas web, consultoría de diseño e implantación de webs e Intranets, etc., etc.)".[306] Resultan interesantes además mencionar las definiciones que la Subsecretaría de Telecomunicaciones de Chile efectuó en la resolución 1.483 de 1999, donde se manifestó que se entiende por el "Servicio de Acceso a Internet como el servicio que permite acceder a la información y aplicaciones disponibles en la red de Internet"; y al "Proveedor de Acceso a Internet, ISP como la persona natural o jurídica que presta el servicio de acceso a Internet, de conformidad a la ley y su normativa complementaria".[307]

Algunas teorías se han tejido en torno al grado de participación y responsabilidad que tienen los ISP cuando por ejemplo, derechos como el de la vida privada de las personas han sido quebrantados. De ello, a mi parecer, deben hacerse ciertas observaciones.

Dentro de quienes proveen del servicio de Internet a los usuarios, están aquellos que lo hacen de manera gratuita. Se ha dado el caso de que, para acceder a este servicio sin costo ofrecido por los ISP, ha sido necesario llenar una serie de datos. De ello se forman grandes bases de datos, y se instalan cookies que permiten seguirle la pista a los cibernautas. El negocio de estos ISP es vender esa información, obtenida de manera ilegal y arbitraria, a terceros. Eso sin duda es atentar contra nuestra vida íntima, y es condenable por la justicia. Para ilustrar lo antes expuesto es interesante mencionar por ejemplo la cláusula sexta del contrato que deben firmar quienes acceden a los servicios gratuitos que ofrece el servidor español EresMás, y que literalmente dice que:

"El usuario presta su consentimiento para que REVISIÓN INTERACTIVA pueda hacer uso de sus datos de navegación por Internet a fin de remitirle, desde el navegador y/o el módulo de software adicional, información y publicidad de terceros". [308]

---

[306] Definición obtenida del Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[307] Considerando 8° del Recurso de Protección N°243-1999 contra ENTEL Chile, en Del Archivo de Gaceta Jurídica, N° 239, pág. 226, edición de Mayo del 2000, Santiago, Chile.

[308] Citado por Carlos SÁNCHEZ ALMEIDA, en España: Intimidad: Un derecho en Crisis. La Erosión de la Privacidad, págs. 4 y 5 de texto publicado en http://publicaciones.derecho.org/redi/No._24_-_Julio_del_2000/20, visitada en enero de 2002.

Un caso distinto es el de los proveedor de servicios que presentan sitios en los que se ofrecen o se cometen actos contrarios al derecho. Común ha sido el caso de Proveedores de Servicios de Internet, donde a través de los sitios que funcionan por los servicios que éstos prestan, se ha injuriado a personas, atentando de esta manera contra su honor y su vida privada. Un caso de estas características se produjo en marzo del año 2000 en Inglaterra, donde el proveedor de servicios *Demon Inc*. fue obligada a pagar, por concepto de indemnizaciones por los daños causados, producto de las injurias transmitidas en un foro de discusión alojado en sus servidores, la suma de 15.000 libras esterlinas. El afectado apuntó la querella contra la empresa proveedora de la conectividad en calidad de responsable editorial de los contenidos injuriosos. [309]

Dentro de la jurisprudencia chilena existe un caso de similares características y que merece ser visto con detalle. Se produjo en Concepción, donde el 31 de julio de 1999, a causa de un aviso que apareció en la sección "Productos y Servicios" que ofrece ENTEL Chile a través de su proveedor de servicios de Internet www.entelchile.net. Dentro de estos "servicios gratuitos" se encuentra la sección de Avisos Clasificados, ubicada en el sitio web http:/www.tribu.cl, administrada por la empresa externa Grupo Web, la que a su vez tiene varias subdirecciones como computación empleos, diversión, espectáculos, etc... Entre ellas se publicó un anuncio de ofrecimientos sexuales en el que figuraba una adolescente de 17 años como remitente y donde se indicaba como teléfono de contacto el de su fono privado. Esto dio lugar a desagradables episodios que produjeron, entre otras cosas, una profunda crisis emocional en la afectada por el mal causado contra su honor y su vida privada. Producto de ello, el padre de la menor decidió interponer un Recurso de Protección contra el ISP, en este caso contra la Empresa Nacional de Telecomunicaciones ENTEL S.A.. Se trata del primer caso en que los tribunales chilenos resolvieron sobre un atentado contra el derecho de la vida privada cometido a través de Internet. De este polémico fallo se concluyó, en resumen, lo siguiente:

"Considerando 19° Que en un sitio web pueden publicarse y divulgarse contenidos ilícitos o nocivos, sean mensajes, avisos o bienes protegidos por propiedad intelectual que no cuenten con autorización cuya utilización cause daño a la honra y bienes de terceros, invadiendo su vida privada e intimidad vulnerando su honra o atentando contra su patrimonio o, incluso, tales avisos o mensajes pueden llegar a ser contrarios a la ley, el orden público, a la seguridad nacional o a la moral o a las buenas costumbres.

En la delimitación de las responsabilidades, son actores en Internet: el proveedor de acceso a la red, el proveedor de sitio o de almacenamiento, el proveedor de contenido y los usuarios o destinatarios finales del servicio.

El proveedor de acceso permite que un determinado usuario se conecte con la red Internet, que de no existir ese acceso haría imposible la comisión del ilícito; el proveedor de sitio o almacenamiento, en la medida que permita que un determinado sitio web en el que se cometan actos ilícitos permanezca almacenando en su

[309]La información de este caso fue obtenida del informe de Renato JIJENA LEIVA, en Responsabilidad de los ISP por la difusión de contenidos on line, págs. 7 y 8. El mismo autor también se refiere a la resolución del Consejo de Telecomunicaciones de la Unión Europea, que el 27 de septiembre de 1996 resolvía que debe impedirse la difusión de contenidos ilícitos en Internet, argumentando que "lo que es ilícito fuera de línea también lo es en línea", enfocando el fallo principalmente a que los Estados Miembros "adopten normas que regulen los nuevos servicios de Internet, en particular la actividad y la responsabilidad de los proveedores de conectividad o suministros de servicios de Internet".

propio servidor, que de no contar con este dispositivo técnico haría imposible la existencia o permanencia de ese sitio web en Internet; y el proveedor de contenido, por ser el que directamente incorpora contenidos ilícitos bajo su tuición en un determinado sitio web."[310]

Para efectos de este caso, y según lo señala el propio considerando 20° de este fallo, ENTEL S.A. tiene a su vez la calidad de proveedor de acceso y de proveedor de alojamiento del sitio http://www.tribu.grupoweb.cl/. La calidad de proveedor de contenido la tiene por su parte la empresa "Grupoweb". De acuerdo al considerando 21°, donde se expone la opinión del Profesor de Propiedad Intelectual de la Facultad de Derecho de la Universidad de Chile y Director General de la Sociedad Chilena del Derecho de Autor, abogado señor Santiago Schuster Vergara, la responsabilidad recae directamente en el usuario proveedor de contenido en la red. Puede además extenderse a aquellos que son incorporados directamente por los destinatarios finales del servicio Internet, cuando el proveedor del sitio ha creado un fondo de información como los foros que en él se encuentran, y no ha tomado las providencias mínimas necesarias para la adecuada identificación de los usuarios que allí participan. Así mismo, se determina que también cabe responsabilidad al proveedor de acceso y al proveedor de alojamiento de la página web respectiva, cuando, a sabiendas de la actividad ilícita que se realiza por los abonados a su servicio, éstos no se han evitado por medio que su acceso se vuelva imposible o que se remueva la información allí contenida. Como lo señala Humberto Carrasco Blanc refiriéndose a este considerando, esta sería la posición que han adoptado algunos países europeos[311],

[310] Considerando 19° del Recurso de Protección N°243-1999 contra ENTEL Chile, en Del Archivo de Gaceta Jurídica, N° 239, pág. 229, edición de Mayo del 2000, Santiago, Chile.

[311]Resulta sumamente interesante conocer la posición de la Directiva de la Unión Europea, que efectivamente parece haber dado las directrices en este fallo. De la mano de la obra de Paula VALLEPUGA GONZÁLEZ se describe a continuación, la posición de los europeos, quienes refiriéndose a la responsabilidad de los ISP, han manifestado que: " Esta Directiva, en principio no impone una obligación de supervisión general; pero para excluirles de responsabilidad regula una serie de imposiciones en función del servicio de la información que presten. La exclusión de obligación general de supervisión se recoge en el artículo 15: *"1. Los Estados miembros no impondrán una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios contemplados en los artículos 12, 13 y 14. 2. Los Estados miembros podrán establecer obligaciones tendentes a que los prestadores de servicios de la sociedad de la información comuniquen con prontitud a las autoridades públicas competentes los presuntos datos ilícitos o las actividades ilícitas llevadas a cabo por destinatarios de su servicio o la obligación de comunicar a las autoridades competentes, a solicitud de éstas, información que les permita identificar a los destinatarios de su servicio con los que hayan celebrado acuerdos de almacenamiento."* La responsabilidad de los distintos prestadores de servicios intermediarios se recoge en los artículos 12, 13 y 14. La Directiva distingue tres tipos de servicios: 1. Servicios de mera transmisión: consiste en transmitir por una red de telecomunicaciones, datos facilitados por el destinatario del servicio o en facilitar acceso a una red de comunicaciones. Estos servicios de mera transmisión engloban el almacenamiento automático, provisional y transitorio de los datos transmitidos siempre que dicho almacenamiento sirva exclusivamente para ejecutar la transmisión en la red de comunicaciones y que su duración no supere el tiempo razonablemente necesario para la transmisión. 2. Memoria tampón o "caching": En este apartado se regula la responsabilidad de los prestadores del servicio de transmisión de datos a través de una red de comunicaciones cuando el almacenamiento de la información es automático, provisional y temporal, realizado además con la única finalidad de hacer más eficaz la transmisión ulterior de esa información a otros destinatarios del servicio a petición de éstos. 3. Alojamiento de datos: consiste en almacenar datos facilitados por el destinatario del servicio. Esta clasificación coincide con la realizada por el Anteproyecto de Ley de Comercio Electrónico español, que ha sido aprobado el 7 de febrero de 2.000. El Anteproyecto los denomina, respectivamente, operadores de redes y proveedores de acceso, prestadores de servicios de almacenamiento de datos y prestadores de servicios de alojamiento de datos. a) Servicios de mera transmisión: los PSIs que ofrezcan este servicio no serán responsables, siempre que: (1) n no hayan originado ellos mismos la transmisión; n no seleccionen al destinatario de la transmisión ; y n no seleccione ni modifique los datos transmitidos. b) "Memoria tampón o caching": no será responsable el prestador de este servicio cuando: (2) n no modifique la información; n el prestador de servicios cumpla las condiciones de acceso a la información; n cumpla las normas relativas a la actualización de la información, especificadas de manera ampliamente reconocida y utilizada por el sector; n no interfiera en la utilización lícita de la tecnología

donde la responsabilidad recaería en los ISP "cuando pueda esperarse razonablemente que son conscientes de que aquel es prima facie ilegal o no han tomado medidas razonables para eliminar dicho contenido una vez que el mismo ha traído claramente su atención."[312]

Sin embargo y a pesar de lo anteriormente expuesto cabe preguntarse si efectivamente los grados de responsabilidad han sido o no correctamente repartidos. Más concretamente, sobre si en realidad en estos caso específicos, los ISP son o no responsables por los actos cometidos contra la vida privada de las personas.[313] A ello ha salido al paso la doctrina chilena, entre ellos Jijena, Carrasco y Llaneza González, quienes argumentan que las exigencias de tomar las "providencias mínimas" como identificar al usuario o extraer contenidos contrarios al orden público, las buenas costumbres o la moral de la red se vuelven técnica y económicamente imposibles de ejecutar por parte de los ISP. Además, no les confiere responsabilidad alguna por su rol de intermediadores. Como lo señala Jijena, "Analógicamente, tal poción sería equivalente al absurdo de sancionar a las compañías de teléfono por permitir a sus usuarios que se conecten con líneas de conversaciones eróticas o pornográficas".[314] En lo personal, comparto las posturas antes mencionadas, ya que

---

ampliamente reconocida y utilizada por el sector, con el fin de obtener datos sobre la utilización de la información; y n actúe rápidamente para retirar la información que haya almacenado, o hacer que el acceso a ella sea imposible, en cuanto tenga conocimiento efectivo de que: Þ la información ha sido retirada del lugar de la red en que se encontraba inicialmente; Þ de que se ha imposibilitado el acceso a esa información; Þ o de que un tribunal o autoridad administrativa ha ordenado retirarla o impedir su acceso a ella. c) Alojamiento de datos (3) : el prestador de servicios no tendrá responsabilidad por los datos almacenados siempre que: Þ no tenga conocimiento efectivo de que la actividad o la información es ilícita y, en lo que se refiere a la acción , no tenga conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito, o;Þ en cuanto tenga conocimiento de lo dispuesto en el párrafo anterior, el PSI actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible. Por tanto, según este artículo, a los servidores que tengan alojadas páginas web no se les obliga a hacer una revisión periódica de su contenido, pero si por cualquier circunstancia conocen que una actividad o información es ilícita deberá o bien retirarla, o bien impedir el acceso a la misma." Esta información fue extraída de la obra Responsabilidad de los Prestadores de Servicio en la Sociedad de la Información, de texto publicado en http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107810, visitado en abril de 2002.

[312] Humberto CARRASCO BLANC, Chile: Algunos Aspectos de la Responsabilidad de los Proveedores de Servicios y Contenidos de Internet. El caso "ENTEL", págs. 6 y 7 de texto publicado en http://vlex.com/redi/No._26_-_Septiembre_del_2000/4, de página visitada en enero de 2002. Este autor cita a su vez a Javier VILLATE por su obra "Censura privatizada: ¿quienes son los editores de Internet?.

[313] Al firmar un contrato por el servicio de Internet con ENTEL en Chile, que por supuesto es un contrato de adhesión, existen una serie de obligaciones del cliente, entre las cuales se encuentran: "No usar la Red Internet o los medios contratados con fines contrarios a la ley, el orden público, o la seguridad nacional, o la moral o las buenas costumbres. Como condición de uso del Servicio, el CLIENTE garantiza a ENTEL que no usará el servicio contratado para cualquier propósito que sea ilegal o prohibido por estos términos, condiciones o demás estipulaciones. Por ejemplo, pero no limitado a, el CLIENTE está de acuerdo en NO USAR EL SERVICIO para: i) Encuestas, concursos, esquemas de la pirámide, cartas de cadena, correos con basura, spamming o cualquier duplicación de mensajes, o mensajes no solicitados (comerciales u otros); ii) Difamación, abuso, amenazas o violación de los derechos legales (como privacidad y publicidad) de otros; iii) Publicar, distribuir, o diseminar cualquier material impropio, profano, difamatorio, obsceno, indecente o ilegal; iv) Transmitir o cargar cualquier material que contenga virus, caballos de Troya, gusanos, bombas de tiempo, o cualquier otro programa dañino." Además existen obligaciones por parte de éste ISP en cuanto a la confidencialidad de la información, estableciéndose que: "ENTEL y sus dependientes deberán mantener en absoluta reserva toda información que obtenga del CLIENTE o que ésta le proporcione en virtud de este contrato; ENTEL CHILE podrá revelar la información confidencial del CLIENTE, sólo en las siguientes circunstancias: Si se entrega a cualquier profesional que trabaja para ella en el grado necesario que permita a esa persona proteger o cautelar los derechos o intereses del CLIENTE, conforme a este contrato y; Cuando la ley lo requiere o sea ordenado por Autoridad competente o por los tribunales de justicia."

[314] Renato JIJENA LEIVA, en Responsabilidad de los ISP por la difusión de contenidos on line, pág. 5.

por las características de la red en estos casos específicos, la responsabilidad recaería en quien comete específicamente el ilícito, a saber el usuario(obviamente siempre que el ISP esté legalmente establecido y no sea éste el responsable de incitar a la comisión de estos ilícitos). El Proveedor de Servicio de Internet no sería sino el "vehículo" que se presta para acceder al ciberespacio, por lo cual de la misma manera que está exenta de responsabilidad una empresa que alquila sin complicidad un vehículo en el cual se comete un crimen, el ISP también debería estar fuera de toda responsabilidad por los ilícitos cometidos en la red. Ello no es impedimento para que, desde mi punto de vista, se imponga a los ISP la obligación de realizar revisiones periódicas respecto de los contenidos que se encuentran en su servidor para que éste no se convierta en cuna de delitos cometidos a través del ciberespacio.

La legislación española, a través del Proyecto Ley de Servicios de la Información y del Comercio Electrónico, más conocida como LSSICE, pretende regular la presencia de contenidos ilícitos en la red, responsabilizando a los ISP en caso de que, al estar al tanto de que su servidor posee algún contenido ilícito, no lo hayan comunicado a la Administración.[315] Es así que dicho proyecto, en el inciso segundo de su tercer punto dice:

"La ley establece, así mismo, las obligaciones y responsabilidades de los prestadores de servicios que realicen actividades de intermediación como las de transmisión, copia, alojamiento y localización de datos en la red. En general, éstas imponen a dichos prestadores un deber de colaboración para impedir que determinados servicios o contenidos ilícitos se siga divulgando. Las responsabilidades que puedan derivar del incumplimiento de estas normas no son sólo de orden administrativa, sino de tipo civil o penal, según los bienes jurídicos afectados y las normas que resulten aplicables."[316] (subrayado es mío).

En todo caso, hay quienes creen que la solución está en que los proveedores de servicio de Internet instalen programas filtro en la red que impidan el acceso a sitios web ilegales. Otros creen que la solución más factible es la autorregulación, o la firma de Tratados Internacionales que regulen sobre el tema.

5.- ¿Las páginas web protegen efectivamente nuestro derecho a la intimidad?

A más de analizar el rol que juegan los Proveedores de Servicio de Internet, es prudente estudiar qué tan efectivas son las políticas de seguridad que los sitios web ofrecen y cómo éstos atentan muchas veces contra el derecho a la vida privada de las personas sin que siquiera nos percatemos de ello.

---

[315] Esta información se obtuvo de una entrevista realizada a la ministra de Ciencia y Tecnología española Anna BIRULÉS, de fecha 3 de diciembre de 2001, y publicada en www.vlex.com y a la cual se puede acceder directamente a través de http://v2.vlex.com/es/asp/noticias_detalle.asp?Articulo=118372, visitada en abril de 2002

[316] Proyecto de Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, o LSSICE, punto tercero, inciso segundo. El texto de esta ley se puede obtener en http://www.libertaddigital.com/suplementos/pdf/anteproyecto_lssice.pdf, visitada en abril de 2002. Este proyecto fue aprobado por el Consejo de Ministros con fecha 8 de febrero de 2002, y en la actualidad ha sido muy cuestionado, sobre todo por grupos que defienden la libertad de expresión.

De hecho, aún cuando existen aparentes garantías frente a la información que uno entrega a estos sitios web, más de uno se ha llevado una sorpresa a la vuelta de la esquina. Para no ir muy lejos, basta con recordar lo polémico que puede ser entregar el número de nuestra tarjeta de crédito, que mal que mal es un dato de carácter personal, a un ente que está al otro lado de la conexión y que no tenemos la menor idea de que efectivamente se trate de quien dice ser. A causa de esto, las estafas en Internet han sido cuantiosas. A ello debe agregársele el hecho de que muchos de estos sitios web también juegan con información que les hemos entregado, comercializándola ilegalmente y sin nuestro consentimiento.

Resulta también curioso que incluso páginas web como Hotmail, (que no solamente ofrecen un servicio de correo electrónico gratuito, sino que tienen una amplia gama de servicios) han transferido datos de sus suscriptores, valiosa información, a un directorio público en Internet.[317] Todavía más polémico es el caso del famoso sitio Terra, que fue multado por la Agencia de Protección de Datos española con la suma de 20 millones de pesetas por haber permitido la fuga de datos personales de sus clientes en agosto del año 2000.[318]

Así mismo, la *American Civil Liberties Unio* (ACLU) habría solicitado en junio de 2001 a la *Federal Trade Comission* (FTC) sancionar a una empresa gigante de productos farmacéuticos, llamada Eli Lilly, por haber divulgado la lista de personas que consumían su antidepresivo *Prozac*. Este hecho ha sido considerado como atentatorio contra el derecho a la vida privada de las personas, pudiendo como consecuencia de ello traer discriminaciones o rechazos contra quienes consumen el fármaco. [319] Un caso más reciente lo protagonizaron Telefónica de España y Telefónica Data, que conjuntamente con Infonegocio.com intercambiaban información de sus clientes creando un banco de datos que se dedicaba a enviar publicidad a sus abonados. Producto de esta práctica ilegal, la Agencia de Protección de Datos procedió a multar a esta empresa de comunicación en diciembre del año 2001 con 140 millones de pesetas por el ilícito cometido. [320]

El caso más alarmante desde mi punto de vista es aquel que se refiere a sitios web que se dedican a entregar información sobre nosotros, vale decir datos de carácter personal e incluso datos sensibles como nombre, dirección, teléfono, cédula de identidad, estado civil, etc... A pesar de que este tipo de páginas no es muy popular en Chile, en Europa y Estados Unidos es pan de cada día. He querido presentar un caso concreto con las siguientes páginas de Internet que prestan sus servicios en Argentina y Estados Unidos respectivamente.

[317] Esta información se obtuvo de la página web de "ciberestrella", con fecha 9 de Marzo de 2001, en donde se manifestaba que "Hotmail cede datos de sus suscriptores a un directorio público de internet". Allí se explica además que "...Hotmail, el servicio gratuito de correo electrónico provisto por Microsoft, está divulgando los datos de sus suscriptores a un directorio público de Internet que cruza esa información con números telefónicos y direcciones...". Para ver el artículo completo, remitirse a http://www.ciberestrella.com/010309/articulos/hotmail.ht5m

[318] El texto completo de esta noticia se encuentra en la página de "Vlex.com", de fecha 4 de abril del 2000, cuyo acceso directo puede lograrse a través de la dirección http://v2.vlex.com/vlex2/front/asp/noticias_detalle.asp?Articulo=101960

[319] Esta noticia se obtuvo de la página web de Newsbytes.com, visitada en abril de 2002. Para ver más detalle de esta información, remitirse a http://www.newsbytes.com

[320] Más información de este caso se encuentra en el diario español El País, en www.elpais.es de diciembre de 2001.

La primera nos permite acceder a correspondencia electrónica de terceros, para de esta manera poder conocer qué mensajes le han llegado al destinatario, cuándo los ha leído, desde qué número IP lo ha hecho, etc.... El reporte se actualiza en tiempo real, y además va informando lo que el destinatario hace. Si al mensaje enviado se le agregan links, el sistema avisa si el destinatario clickea en los mismos. La segunda, como se lee en ella, revela por una suma de dinero, información “demasiado” completa sobre nuestra vida personal.

EL SUPER BUSCADOR ARGENTINO (Nueva Version)

Necesita buscar información sobre personas?
Le presento un exclusivo buscador de información que recorre sitios publicos y encuentra el dato que usted esta buscando.

El sistema busca y encuentra :

* documento * cuit * domicilio * localidad * provincia * teléfono/s * empleo * obra social * sexo * fecha de nacimiento * estado civil * actividad * art * teléfono art * fax art * cuit empleador * denominación empleador * domicilio empleador * código postal empleador * deuda en entidades bancarias (entidad, situación, monto) * Inscripción en monotributo (categoría , actividad , fecha de inscripción) * Inscripción en IVA * Cheques Rechazados (Numero, fecha del rechazo , monto, causal , denominación, fecha de pago) * Facturas Apocrifas * Si tiene Empleados y quienes son * Incumplidores Fiscales (con Causas Penales, con Ejecuciones Fiscales, con Clausuras, con Incumplimiento en IVA y Seguridad Social), etc, etc, etc
Recuerde: toda esta información es de acceso publico, solo nuestro buscador sabe donde encontrarla .
Busque por documento o apellido y nombre. Aplique Filtros y ordene la informacion.

Nuestro sistemas busca y acumula toda la información que encuentre, luego la agrupa en una sola pagina web para que usted visualice el resultado cómodamente .

VA A SEGUIR PAGANDO LOCURAS POR ESTA INFORMACIÓN ??? OLVIDESE!!!

Y lo mas Importante: La informacion no reside en el sistema, por lo tanto el sistema no se actualiza, los sitios webs donde se accede mantienen actualizada su informacion. Ademas: Si detectamos nuevos sitios con información publica le actualizamos el sistema gratuitamente por un año .

Imperdible: **Solo $60** **(POR UNICA VEZ! NO ES ABONO)** (Gastos de envio a todo el pais incluidos, usted lo abona contrareembolso)

ATENCIÓN: Compre 3 o mas copias y obtenga el sistema a un 50% de su valor.

Contactenos sin compromiso. Respondemos todas las consultas!!!

Solicite telefonicamente el sistema de 9hs a 22hs al: 0343 15 504 7496

O con ICQ al UIN 145872191

para ser removido de nuestra base de datos envie un email vacio a noenviarmas@uol.com.ar

No tiene ICQ? Bajelo haciendo click aqui

Como consecuencia de la indiscriminada transferencia de datos de carácter personal que se efectúan a través de Internet, ya algunos ordenamientos jurídicos están tomando cartas en el asunto. Resulta interesante mencionar un pronunciamiento de la Unión Europea, donde en diciembre del 2001 se manifestaba en Bruselas que: "El Consejo de Ministros de Telecomunicaciones de la Unión Europea ha alcanzado un acuerdo sobre la Directiva referente a la privacidad en las comunicaciones electrónicas, norma que compromete a organismos públicos y privados a destruir o hacer anónimos los datos personales que obtengan a través de sus comunicaciones en Internet, excepto si consideran que éstos afectan a la seguridad pública o del Estado". Uno de los grande aportes de este hecho constituye el reconocimiento que la Directiva establece al principio universal de la "destrucción inmediata" de los datos personales. Es así que se permite almacenar tales datos si el usuario ha sido informado. Sin embargo, esta destrucción no se llevará a cabo "si fuera necesario para la protección de la seguridad pública, la Defensa, la seguridad del Estado, incluido el bienestar económico, o la aplicación del ordenamiento penal".

Se dice que esta norma no altera el equilibrio actual que las legislaciones nacionales mantienen entre el derecho a la intimidad y la protección de la seguridad. Esta nueva legislación, que tiene como objeto mantener el nivel de protección de la vida privada ante la irrupción de nuevas tecnologías de la comunicación, fue aprobada después de que los ministros resolviesen los últimos puntos de fricción de la propuesta original, en especial, el referido al correo electrónico publicitario con fines de venta, que, como norma general, no podrá ser enviado sin autorización previa del receptor. [321]

A nivel latinoamericano, no hay todavía nada concreto en cuanto a afrontar este problema. Pero debemos sin lugar a dudas servirnos el día de mañana de la experiencia legislativa de otros países que en la actualidad ya se encuentran luchando contra los peligros que traen consigo las nuevas tecnologías.

6.- Internet como medio de control del empleador sobre el trabajador:

Es difícil que en estos días una empresa de tamaño mediano a grande no se encuentre incorporada a los servicios que le ofrece Internet. De hecho, es de todos conocido que con la llegada del ciberespacio, el mundo laboral sufrió grandes transformaciones, ya que esa necesidad imperiosa de contactarse con gente, conocer otros mercados, sobrepasar fronteras, ofrecer sus productos a nivel nacional e internacional, palpar las tendencias de la economía, transar en las bolsas de cualquier parte de la Tierra, por nombrar algunas ventajas, se volvió una realidad para muchos sin necesidad de ser grandes potentados económicos. Internet abrió las puertas del mercado al mundo. Sin embargo, quienes en la actualidad se han dedicado a estudiar el fenómeno de la red respecto del impacto que produce en la vida privada de las personas están especialmente preocupados por la amenaza que se ha vuelto este medio de comunicación a la hora de controlar a los empleados. Es por ello que hemos querido tratar este caso que, si bien tiene similitud con puntos analizados

[321] Esta noticia puede leerse con detalle en artículo publicado por www.elmundo.es de fecha 7 de diciembre de 2001, titulado "Decisión de los ministros de telecomunicaciones. La UE respetará la privacidad de datos en Internet salvo cuando afecten a la seguridad", que fuera visitado en abril de 2002. Para acceder directamente a este artículo, remitirse a http://www.elmundo.es/navegante/2001/12/07/seguridad/1007715325.html

anteriormente, merece ser estudiado por el alcance que está logrando a nivel mundial. Se trata pues nuevamente de dos derechos constitucionales en conflicto. El primero de ellos, el derecho a la libertad de trabajo y su protección, la libertad de empresa y la libertad de información; y el segundo, el derecho a la vida privada de las personas. Este aparente conflicto se traduce en la vida cuotidiana en distintas circunstancias.

Al momento de contratarse a personal, se suele hacer un proceso de selección, legítimo en los casos en que éste se vea fundado en capacidades, aptitudes y condiciones laborales del postulante. Para ello se utilizan distintos mecanismos como currículos, entrevistas, pruebas, tests, e incluso la contratación de empresas que se encargan de esto. Sin embargo, en este proceso de búsqueda de información del potencial trabajador, se puede llegar a la averiguación de datos que se consideren personales en incluso sensibles, y que pueden amenazar la vida privada del postulante, como por ejemplo su tendencia política, su religión, su estado de salud, su capacidad económica, etc... Este tipo de antecedentes pueden ser de gran importancia para el empleador, ya que puede revelarían valiosa información a la hora de programar el pago de imposiciones, o su posible grado de participación sindical, su estado de salud, por nombrar algunos ejemplos. Sin embargo, si ésta se obtiene a través de medios ilícitos como la transferencia de datos de carácter personal a través de Internet sobre una persona, sin que existiera previamente la prestación de su consentimiento, obviamente que se trata de un acto de discriminación ilegítimo. [322]

Pero uno de los casos que más ha llamado la atención es el uso de la red como medio de control del empleador sobre el trabajador. Se discute básicamente si Internet es una herramienta lícita para inspeccionar a los subordinados o si en realidad se está atentando contra la intimidad de éstos. El problema se da básicamente a la hora de determinar si es legal que el empleador revise, por ejemplo, la correspondencia electrónica de sus empleados, y por consiguiente examine también hechos pertenecientes a la vida privada de éstos. ¿Se puede despedir al trabajador por concepto de la información que se obtuvo al examinar su correo electrónico?

Uno de los casos de mayor impacto al respecto se produjo a finales del año 1999 en España, donde un empleado del Deutsche Bank fue despedido luego de que se demostrara que usaba el correo electrónico que le otorgara la empresa para fines distintos a los que se le había asignado. La defensa de Gregorio Giménez Román, el empleado despedido, tuvo sus fundamentos en que se violó su correspondencia y por consiguiente se atentó contra su vida íntima al habérsele revisado su casilla de correo electrónico. Por su parte , el banco legitimó su defensa en el hecho de que el ex empleado utilizaba el correo de la empresa en forma improcedente y masiva para enviar mensajes a través de Internet, muchos de ellos con contenido pornográfico. El afectado recurrió ante el Juzgado de Instrucción Segundo de Barcelona, y posteriormente

---

[322] Para ver con más detalle este tema, remitirse a la obra de José CUERVO, La Intimidad Informática del Trabajador, pág. 8 de texto publicado en http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=106971, visitado en enero de 2002.

ante el Tribunal Superior de Justicia de Catalunya, que a su vez legitimó el proceder del Deutsche Bank, argumentando que "concurre así un acreditado incumplimiento laboral del trabajador sancionado, ya que su actitud supone la pérdida de tiempo de trabajo efectivo, tanto del trabajador al confeccionar y enviar los mensajes como de sus compañeros al recibirlos y leerlos". El informe de la Fiscalía de Catalunya sentenciaba además que: "el derecho a la intimidad es aplicable al ámbito de las relaciones laborales pero en dicho ámbito debe tenerse en cuenta que el poder de dirección, imprescindible para la buena marcha de la organización productiva, atribuye al empresario, entre otras facultades, la de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones laborales". El único límite que pone la fiscal a ese control es que el empresario debe ejercer esas facultades "dentro del debido respeto a la dignidad del trabajador" . Según los abogados del banco, la empresa había advertido a sus empleados de la naturaleza exclusivamente profesional que debía tener el uso del correo electrónico.[323]

Otro caso de similares características se produjo también en España, en diciembre del 2001, luego de que una empresa, Productos Eaton Livia, instalara un programa informático en los ordenadores de los trabajadores para controlar tanto sus actividades como su rendimiento laboral. Producto de ello, se despidió a un empleado que había estado jugando solitario desde su puesto de trabajo. En primera instancia, un Juzgado Social de Barcelona había dado la razón al trabajador. Sin embargo, el Tribunal Superior de Justicia de Catalunya revocó el fallo, alegando que "el ordenador es un instrumento de trabajo que pertenece a la empresa y un medio al servicio de los fines económicos y mercantiles de la misma y que el empresario tiene todo el derecho a supervisar la actividad de sus empleados". La compañía, según la sentencia, instaló los programas de control de forma que no pudieron ser detectados por el usuario y lo hizo sin entrar en el PC del trabajador por lo que, según destaca el tribunal, no violó su password (código de acceso), y que se trataría de un programa que se activaba de forma automática cuando se ponía en marcha el ordenador. Así mismo, el veredicto indicaba que de acuerdo con el control de la empresa, el empleado se pasó un día jugando menos de una hora, durante otros seis días estuvo entre una hora y dos, durante otros 24 días estuvo entre dos y tres horas y dos días más jugó más de tres horas. El "programa espía" tenía la particularidad de identificar los programas y ventanas de Windows que se activaban en cada momento sin invadir los contenidos, ni siquiera el PC. En conclusión, para el Tribunal Superior de Justicia de Catalunya, la medida de control informático de la empresa era "justificada (ya que existían razonables sospechas de la comisión por parte del empleado de graves irregularidades en su puesto de trabajo)".[324]

Frente a los dos casos recién expuestos, es preciso reflexionar acerca de la legalidad de los métodos utilizados por el empleador a la hora de controlar a sus trabajadores. En lo personal, creo que las personas tenemos vida privada donde quiera que nos encontremos, ya sea en nuestra casa, en nuestro trabajo, en nuestro automóvil o

---

[323] La información de este caso se obtuvo de http://www.elmundo.es/navegante/2001/11/26/esociedad/1006801495.html de fecha 26 de noviembre de 2001, en artículo titulado "CATALUÑA / CORREO ELECTRÓNICO La Fiscalía entiende que no es delito que los jefes controlen los 'e-mail' de sus empleados", visitado en abril de 2002.

[324] Esta información se obtuvo de la dirección electrónica española de www.noticias.com , de fecha 5 de diciembre de 2001.

mientras estamos de vacaciones. Por consiguiente, nuestra correspondencia, que forma parte de nuestra esfera íntima, debe ser respetada igualmente. Sin embargo, creo que debemos ser concientes que el computador, así como por ejemplo el fax o el teléfono son bienes que le pertenecen a la empresa y que tienen asignada una función determinada para su uso, cual es el funcionamiento de ésta. De ello se desprende que toda función que se le de a estos accesorios y que sea contraria con los fines para los cuales se le facilitó al trabajador constituyen causales de incumplimiento de los deberes laborales. Veo razonable que, dentro de las cláusulas del contrato de trabajo, se especifique que por ejemplo el correo electrónico que la empresa otorga a sus trabajadores no es de uso personal, sino profesional, y por consiguiente sea perfectamente posible que el empleador lo examine siempre que crea necesario. Además, compartiendo la postura de gran parte de la doctrina sobre este asunto[325], de requerirse el inspeccionamiento del mismo, éste debería llevarse a cabo previa notificación al trabajador, indicándole el motivo de la inspección y qué se va a inspeccionar (obviamente todo ello debe practicarse con fines puramente profesionales). Dicha notificación no necesariamente debe significar avisar con tiempo de la inspección que se va a realizar (ya que en este caso se corre el riesgo de que puedan cometer fraude los trabajadores), sino que la notificación debería interpretarse más como el hecho de efectuar tal revisión de la casilla en presencia del trabajador.

Resulta interesante la opinión del juez norteamericano James M. Rosenbaum, quien en una entrevista concedida al diario argentino Clarín[326] en diciembre del 2001 señalaba que: "Ha surgido un nuevo "principio legal". Si una corporación, empresa u organismo del Estado posee una computadora y un empleado pone en ella cosas personales, el autor no tiene derecho sobre el material almacenado ni puede esperar privacidad". Según el magistrado, los estadounidenses sienten una profunda repulsión por las "inspecciones generalizadas"[327]. Continua el juez argumentando que "si no se le da el debido aviso al trabajador de que se va a llevar a cabo una inspección, el empleador debería perder todo derecho a tomar cualquier medida laboral adversa al trabajador".

Dentro de la jurisprudencia chilena, un dictamen de la Dirección del Trabajo señalaba que "en ningún caso el empleador puede ingresar a la correspondencia privada que reciben o envían sus trabajadores, pero tiene la

---

[325] Una detallada exposición de este tema está en la publicación de Rodolfo HERRERA BRAVO en Chile, España: La Legitimidad del Control Tecnológico del Empleador sobre el Trabajador, que puede obtenerse en http://vlex.com/redi/No._35_-_Junio_del_2001/4, visitada por el autor de este trabajo en enero de 2002.

[326] Esta información se obtuvo de la Columna de Opinión del diario argentino Clarín de fecha 5 de diciembre de 2001, en entrevista al Juez del estado de Minnesota, James M. ROSENBAUM, en un artículo titulado "Ante todo, privacidad".

[327] El precedente del tema que se trata en esta entrevista es el siguiente: "Hace unos meses, este tema se planteó en las oficinas de una importante editorial neoyorquina. Un gerente de la oficina comercial de la empresa recibió un sobre que contenía material fotocopiado. Cualquiera fuera el contenido, al gerente le resultó claramente ofensivo. La empresa reaccionó con una búsqueda clandestina en la división "infectada" revisando el contenido del disco rígido de todas las computadoras, sin avisar a los empleados y pese a que el material ofensivo había sido fotocopiado y no generado por una computadora. Según parece, la búsqueda descubrió una serie de elementos irritantes que iban desde chistes hasta pornografía, todos dentro de computadoras de la empresa. La consecuencia: alrededor del 10 por ciento de los empleados del departamento fue despedido, otros fueron reprendidos". La información de este caso se obtuvo de la misma entrevista efectuada por el diario Clarín de fecha 5 de diciembre de 2001 al juez ROSENBAUM, cuyo texto fue extraído de la Columna de Opinión del mencionado diario.

facultad de regular las condiciones, frecuencia y oportunidad de la utilización de los mail que puso a disposición de sus empleados". Según palabras del subdirector del Trabajo Marcelo Albornoz, "Esta resolución se basa en dos derechos constitucionales comprometidos: asegurar la privacidad de las personas y, por ende, la de los trabajadores; y por otro lado, estamos en presencia del derecho del empleador de resguardar su propiedad". El subdirector es partidario de que para el control de estos instrumentos de comunicación, lo más adecuado sea regirse por un reglamento interno o a través de contratos individuales y colectivos. Para evitar una utilización exagerada, se propone igualmente el uso de mecanismos de control, en común acuerdo con los trabajadores, y un ejemplo de ello es que los trabajadores envíen una copia de todos los correos que formen parte de su labor o funciones para las cuales fueron contratados, remitida a la gerencia o a la unidad de control a la cual dependan. Como conclusión, se argumenta que el empleador puede controlar el ingreso o salida, acceso y el número de correos, pero no puede entrar a conocer su contenido.[328]

Desde mi punto de vista, debe precisarse que si es la empresa la que provee de computadores a los trabajadores, y si ésta además les entrega una casilla de correo electrónico que incluso lleve dentro de la dirección el nombre de dicha entidad (ejemplo: fcoronel@entel.cl), es precisamente la empresa la dueña de la casilla. Se trata de un bien que ésta entrega a sus miembros para el desarrollo de las actividades para las cuales han sido contratados. En este caso, el trabajador no es más que un usuario de un bien que le pertenece a la persona jurídica, de la misma manera que el vehículo que por ejemplo determinados empleadores les facilitan a sus trabajadores para el desarrollo de sus actividades laborales. Se vuelve además indispensable, creo yo, para evitar posibles arbitrariedades, que dentro del contrato de trabajo se especifique con toda claridad cuales son los márgenes dentro de los que deben manejarse los trabajadores al hacer uso de los bienes que le pertenecen a la empresa, en este caso específico, el correo electrónico que ésta les facilita. Dentro de la doctrina nacional, el profesor José Joaquín Ugarte Godoy comparte también esta postura.

De lo anteriormente expuesto, se puede además deducir que se trata de otro argumento legítimo que tiene el empleador, que apegado a las normas de derecho, le podría permitir inspeccionar las casillas de correo electrónico de sus subordinados.

7.- Internet y los Órganos Gubernamentales:

Muchos entes policiales e investigativos utilizan Internet, concientes de que es una poderosa herramienta al momento de realizar sus labores. Para los servicios de inteligencia, se trata de un medio sumamente útil y necesario para transmitir y recabar información. De esta manera, una nueva función de la red ha ido tomando forma, es lo que muchos expertos han llamado el *ciberespionaje*.[329]

---

[328] Esta información se obtuvo del diario Últimas Noticias de Chile, de fecha 2 de marzo de 2002, y se encuentra en la siguiente dirección de Internet: http://www.lun.cl/librerias/prt_em.asp?idnoticia=C37289942337963

[329]La palabra *cyber* o ciber se define como un "Prefijo utilizado ampliamente en la comunidad Internet para denominar conceptos relacionados con las redes (cibercultura, ciberespacio, cibernauta, etc.). Su origen es la palabra griega *kibernao*, que significa pilotar una nave". Definición obtenida de Glosario de Términos Informáticos en

Y es que efectivamente, la red muchas veces ha sido utilizada como medio para la comisión de ilícitos como crímenes, narcotráfico, e incluso actos terroristas. Sin ir muy lejos, recordemos que mucha información para cometer los atentados del 11 de septiembre fue transmitida a través de páginas de Internet, donde por medio de ciertos links[330], se revelaba información para cometer estos actos, como por ejemplo los planos de un avión, indicaciones precisas del actuar de los terroristas, etc... Ello ha motivado a que órganos gubernamentales, para contrarrestar este tipo de actos, utilice a su vez la red para rastrear el uso que los particulares hacen de ella.

Con el fin de ilustrar esto, he querido reproducir un extracto de una noticia que señalaba que: " Carnivore, la controvertida herramienta de vigilancia de mensajes de correo electrónico desarrollada por el FBI puede tener acceso a todo tipo de comunicaciones enviadas a través de Internet, según pruebas recientes. Un oficial del FBI que participó en las pruebas señaló que aunque Carnivore tiene la habilidad de grabar una gran cantidad de mensajes de correo-e y otro tipo de comunicaciones vía Web, su uso está restringido por las leyes y las ordenes específicas de los tribunales.

Por su parte, Marcus Thomas, jefe de la sección de cybertecnología del FBI, declaró que en una situación real, la herramienta no podría ser usada para capturar todo tipo de comunicaciones en Internet. "Ciertamente, en una operación, podrías poner a los filtros para que hagan nada. Pero nuestros procedimientos son muy detallados, solamente hacemos lo que nos está permitido por la orden de la corte", añadió Thomas."[331] Sin embargo, aún cuando en teoría estos mecanismos de rastreo debieran ponerse instalarse solamente previa autorización por parte de la autoridad competente, en la práctica esto no sucede, y es de todos sabido.

Países como Estados Unidos han propuesto la creación de una *ciberpolicía*, que como lo explica el español Sánchez Almeida, se trataría de "un cuerpo de intervención rápida que pudiese actuar en cualquier país del mundo sin autorización judicial, a fin de perseguir el cibercrimen allí donde ocurra". Agrega que "La prensa ha explicado que los países europeos lo han evitado, vendiendo la imagen de que Europa es más respetuosa con los derechos fundamentales. Tal información es tendenciosa". [332] Efectivamente, el control de la red es una tarea muy difícil de lograr, por no decir imposible. Aún cuando existen entes como el famoso ECHELON (conocido también por las siglas UKUSA, y que es un sistema de escuchas y filtrado de conversaciones a través del teléfono o de Internet), los gobiernos no van a dar su brazo a torcer en este campo. Sánchez

---

http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002. De esta raíz es que se ha formado el término *ciberespionaje.*

[330] Se lo define así: "*link* (liga, puntero, vínculo/vincular,*enlace/enlazar*) Apuntadores hipertexto que sirven para saltar de una información a otra, o de un servidor a otro, cuando se navega por Internet o bien la acción de realizar dicho salto." Definición obtenida de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[331] Citado por Renato JIJENA LEIVA, en Chile: "Internet, Privacidad y Derecho": Un desafío de cara al siglo XXI en el marco de la globalización, págs. 9 y 10 de texto publicado en http://vlex.com/redi/No._36_-_Julio_del_2001/3, visitado en enero de 2002.

[332] Carlos SÁNCHEZ ALMEIDA, en España: Intimidad: Un derecho en Crisis. La Erosión de la Privacidad, pág. 4 de texto publicado en http://publicaciones.derecho.org/redi/No._24_-_Julio_del_2000/20, visitada en enero de 2002.

Almeida, refiriéndose a estos órganos argumentaba que "Mucho se ha hablado sobre ECHELON: gracias a los descubrimientos del periodista Duncan Campbell, fue objeto de un debate reciente en el Parlamento Europeo. Curiosamente, ese mismo Parlamento aprobó el 7 de mayo de 1999 el proyecto ENFOPOL, un sistema que pretendía que la Red pudiese ser transparente a la investigación policial. En las bases técnicas de Enfopol se habla de que todas las comunicaciones, origen, destino, contenido de los mensajes, puedan disponerse en tiempo real por la "autoridad competente". Afortunadamente, y espero no equivocarme, las sucesivas movilizaciones de grupos de defensa de derechos civiles van teniendo efecto, y el proyecto se está convirtiendo en un acuerdo de colaboración en el ámbito estrictamente judicial, que requerirá en cualquier caso autorización de los tribunales para cualquier tipo de escucha. Con todo, habrá que mantener la guardia".[333]

Sin embargo, el problema está en que la información que estos servicios perciben muchas veces ha sobrepasado los límites puramente investigativos y se vuelven verdaderos sistemas de persecución que atentan contra el derecho que todo ser humano tiene para no ser perturbado y para que no se conozcan aspectos de su vida que se consideren como íntimos. Es prudente que los Estados, que legítimamente pueden crear órganos para combatir delitos que se cometan con o sin participación de medios de comunicación como Internet, alcancen al momento de desempeñar sus funciones, un equilibrio armonioso entre el legítimo derecho a investigar este tipo de crímenes y el derecho a no intervenir en la vida privada de las personas. Pero en la práctica, estas expectativas parecen poco alentadoras.

A través de los casos recientemente expuestos, surge por de pronto una controversia entre algunos derechos constitucionales, vale decir el derecho a la protección de la vida privada y otras garantías como el derecho a desarrollar actividades económicas o el derecho a la propiedad privada, y que se encuentran básicamente arraigadas en quienes desarrollan actividades económicas al parecer lícitas.

Ya a finales del siglo XIX, los connotados Warren y Brandeis se habían manifestado respecto de las controversias que tales derechos acarreaban, producto de que muchas veces se falló dando prioridad más a la propiedad que a la privacidad. Por eso es que daban como ejemplo el hecho de que "el principio que protege los escritos personales y toda otra producción personal, no contra el robo o la apropiación física, sino contra toda forma de publicación, no es en realidad el principio de la propiedad privada, sino el de una inviolable personalidad"[334]. Pero en la actualidad, el problema ha tenido tanto defensores como detractores.

Dentro de quienes defienden a la vida privada como un bien económico que todos tenemos conjuntamente con otros, está el profesor de la Universidad de Chicago Richard Posner. Para este autor, estos dos bienes no son entendidos como fines en sí mismos, sino como bienes intermedios para lograr otros fines. Desde esta

[333] Ibídem.

[334] Citado por Hernán CORRAL TALCIANI, (refiriéndose a la obra de Richard POSNER, The Right of Privacy, en Giorgia Law Review, 12(3), 1978, p394)en Configuración Jurídica del Derecho a la Privacidad II, de texto publicado en Revista Chilena de Derecho, Vol. 27 N°2, pág. 354, Sección Estudios.

perspectiva, el chileno Hernán Corral la ha descrito así: "la "demanda por información privada" es comprensible cuando una relación actual o potencial, sea comercial o personal, crea oportunidades de ganar para el demandante, lo que es obvio para el inspector del Servicio de Impuestos, para el novio, para el conviviente, acreedor y competidor, entre otros buscadores de información. Incluso estima comprensible la curiosidad casual por las vidas de amigos y colegas, ya que ella nos permite formarnos una imagen más adecuada de aquellos, y el conocimiento así obtenido es útil en nuestro trato social"[335].

La postura de Posner se sintetiza, básicamente enfocando al derecho a la vida privada sustentado en la eficiencia económica (donde la gente se vendería a sí misma tanto como a sus bienes), y según los siguientes principios: "1) otorgar protección a los secretos de negocios o comerciales por los cuales los hombres de empresas explotan su superior conocimiento o habilidades; 2) no conceder, en general, esa protección a los hechos personales de la gente como mala salud, mal carácter, sobre los cuales no podrá otorgarse un derecho de exclusividad, aunque sí para prevenir su descubrimiento mediante métodos indudablemente intrusivos; 3)limitar, tanto como sea posible, las escuchas comunicacionales y otras formas de vigilancia intrusiva a la vigilancia de actividades ilegales".[336]

Dentro de los detractores de esta postura está Edward Bloustein, quien ha manifestado que el hecho de que el secreto incentive la inversión en la producción de una información socialmente valiosa, se sale del campo meramente económico para expresar un juicio de valor. Así, el estudio de Posner no lograría capturar el significado de la privacidad como un valor final, y no como un instrumento meramente económico: "el mercado nos dice algo sobre la realidad social, pero está lejos de decírnoslo todo, y frecuentemente, está lejos de decirnos lo suficiente".[337]

Considero prudente, a modo de reflexión, tomar las palabras del propio profesor Corral, quien a modo de conclusión ha manifestado que "La información personal no puede ser objeto de propiedad en la medida en que no se trata de un objeto ni tangible ni intelectual, y porque su grado de proximidad a la persona misma le otorgan una calidad personalísima que la extrae de las categorías de la comercialidad y del tráfico del mercado"[338]. Soy partidario de la postura recién manifestada, ya que no se puede, desde mi punto de vista, poner en riesgo bajo ninguna perspectiva una garantía esencial del hombre por dar cabida a intereses que no se equiparan ni en importancia ni en prioridad respecto de la esencia misma del hombre. Es a raíz de esto que

[335] Ibídem. Dentro de esta postura están incluso aquellos que sostienen que aquella información basada en chismes típica de la prensa sensacionalista tiene también su justificación. "Hay aparentemente muy poca privacidad en las sociedades pobres, donde, consecuentemente, la gente puede fácilmente observar a de primera mano la intimidad de la vida de los otros. La vigilancia personal es un lujo en las sociedades ricas, porque la gente vive en condiciones que les proporcionan altas cotas de privacidad de tal observación y porque el valor (y por tanto el costo de oportunidad) del tiempo es mayor – demasiado grande para merecer una asignación de tiempo para mirar a los vecinos. La gente de las sociedades ricas vio un método alternativo de informarse sobre cómo viven los demás y la prensa lo proveyó. Una función legítima e importante de la prensa es proveer especialización de la curiosidad en las sociedades donde los costos de obtener información han llegado a ser demasiado altos para el fusgón."

[336] Citado por Hernán CORRAL TALCIANI,en Configuración Jurídica del Derecho a la Privacidad II, de texto publicado en Revista Chilena de Derecho, Vol. 27 N°2, pág. 72, Sección Estudios.

[337] Ibídem, refiriéndose básicamente a la obra de Edward Bloustein, Privacy es dear al any price: a response to professor Posner's Economic Theory, en Georgia Law Review 12, 1978, p440.

[338] Ibídem, pág 72.

se ha desarrollado en la actualidad justamente una fundamentación postmoderna, inclinada por sobre todo a la defensa de la dignidad humana frente a la amenza que representan los intereses económicos en este campo. Bien ha dicho Bloustein que "la autoestima que aflora del derecho a la vida privada es un valor único y no susceptible de cambio"[339]

[339] Ibídem, pág73.

CAPÍTULO VI: EN BUSCA DE SOLUCIONES PARA PROTEGER EL DERECHO A LA VIDA PRIVADA FRENTE A LAS NUEVAS TECNOLOGÍAS

Uno de los principales desafíos que tiene el legislador frente a la llegada de nuevos y poderosos medios de comunicación es velar por una armoniosa convivencia entre la tecnología y los derechos fundamentales del hombre, para que de esta manera, un avance de la ciencia no se transforme en un retraso para el derecho. Lamentablemente, en el mundo actual muchas veces ha quedado demostrado que las políticas de desarrollo económico han podido más que aquellas políticas tendientes a proteger la esencia del hombre en sí, de lo que es suyo por naturaleza, de proteger sus derechos y su vida. Desde esta perspectiva, garantías fundamentales como el derecho a la intimidad han sufrido constantes amenazas. De esto son concientes incluso los que podrían considerarse "padres de la tecnología" de estos tiempos, entre ellos Bill Gates, quien ha manifestado que: "Proteger la privacidad individual es la mayor barrera que debe ser removida lo antes posible para mantener a Internet en movimiento hacia adelante. Mantener una Internet Segura. La seguridad es siempre el mayor asunto para los empresarios y gobiernos, se sustenta en la confianza en las TI (Tecnologías de Información) y siempre será así. Esto es también verdad para la seguridad de los individuos".[340]

Frente al reto que tenemos por delante las futuras generaciones, muchas teorías para afrontar esta amenaza han surgido, algunas más lógicas y factibles de aplicar que otras. A continuación, haré una breve exposición de las soluciones que más se discuten en la actualidad para frenar el fenómeno de Internet. Para una comprensión más completa, es preciso desde mi punto de vista que, sean expuestas desde dos perspectivas: una tecnológica y otra jurídica.

Soluciones Técnicas

Así como muchos han visto en la tecnología un camino grandioso al momento de mejorar nuestra calidad de vida, han apuntado a que a través de la propia tecnología es posible solucionar las deficiencias que su implementación trae consigo. Esta postura ha dado pie a las siguientes propuestas:

1.- El Proyecto Plataforma para Preferencias de Privacidad o P3P:

Este proyecto tiene su origen en un estudio que pretende que los sitios web ofrezcan políticas de protección a la intimidad de sus usuarios, y que ellos manifiesten el grado de intimidad que requieren se les

[340] William H. GATES, Ensayo para el Presidente de Estados Unidos, texto publicado de www.emol.cl con fecha 8 de febrero de 2001, visitado por el autor de este trabajo en la misma fecha.

aplique al hacer uso de la red. Es así que en mayo de 1998, el *Word Wide Web Consortion*, o W3C[341] presentaba este protocolo de privacidad, conocido como P3P.

En cuanto al funcionamiento de este sistema, Javier Villate lo describe de la siguiente manera: "El usuario define cuáles son sus preferencias de información de sus datos personales. De acuerdo con ellas, un agente de usuario emprenderá una serie de acciones cuando se conecte a un sitio web. El agente de usuario puede residir en el propio ordenador del usuario o en el del proveedor del servicio. El sitio web, por su parte, debe expresar cuáles son sus prácticas de privacidad. A partir de ese momento, el agente de usuario y el sitio web establecen una negociación (envío de preguntas y respuestas) con el fin de llegar a un acuerdo respecto al intercambio de información. En teoría, el usuario podrá dar su conformidad a los términos del acuerdo alcanzado e iniciar la exploración del sitio web, o bien rechazarlo, en cuyo caso le será denegado o restringido el acceso a este último."[342]

Sin embargo, muchas dudas en cuanto a su efectividad han surgido, y una de ellas es que, según el profesor de la Facultad de Derecho de la Universidad de Miami Jeremy Birchman, "una vez que el usuario especifica sus preferencias de privacidad, todo el proceso escapa a su control (...) el usuario entrega el control a un agente de usuario". De ello se desprende que no existiría ninguna garantía en cuanto al adecuado funcionamiento de los acuerdos entre esta entidad y sus usuarios. A más de esto, surgen interrogantes lógicas como ¿qué sucede si por ejemplo se comete un ilícito por parte del *agente de usuario*?, y de suceder esto, ¿ante qué órgano, entidad o tribunal se debe recurrir?

2.- El sistema *Opt-in*:

Como se explicaba anteriormente, se trata de un sistema que requiere, al igual que el anterior, de la autorización del usuario al momento de hacer uso de sus datos de carácter personal. Se trata en definitiva de una autorización explícita para el manejo de datos de estos datos. Este sistema ha sido adoptado por algunos organismos, como el Departamento de Comercio de la Unión Europea, frente a la negociación de transmisión de datos a los Estados Unidos.

Otro caso en que este sistema ha tenido aplicación es a través del Consejo de Ministros de Telecomunicaciones de la Unión Europea, que aprobó una regulación del uso de comercio electrónico no deseado, inclinándose por este sistema *Opt-in*.[343]

---

[341] El Glosario de Términos Informáticos ha definido a *W3 Consortium* o W3C (Consorcio W3) como la " Organización apadrinada por el MIT y el CERN, entre otros, cuyo cometido es el establecimiento de los estándares relacionados con WWW. Fue promovida por el creador del WWW, Tim Berners-Lee". La dirección de dicho glosario se encuentra en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[342] Javier VILLATE, P3P, un estándar para la privacidad. ¿Es lo que necesitamos?, pág. 1 de texto publicado en http://vlex.com/redi/No._01_-_Agosto_de_1998/villate, visitado en diciembre de 2001.

[343] Para ver más sobre esta noticia, remitirse a la nota 299, que se encuentra en el capítulo V de este trabajo.

A contrario sensu, el sistema *Opt-out* ha sido rechazado prácticamente en forma unánime, y consiste en que se da al usuario la posibilidad de prohibir el uso de sus datos personales sólo cuando éste resulte contrario al propósito para el cual fueron recolectados. Esto quiere decir que se tiene por asumido que la autorización del usuario existe. Este sistema ha sido defendido por muchas empresas, pero en la práctica se ha visto reflejado en constantes abusos por parte de quienes lo han adoptado.

3.- Los Certificados de Garantía y los llamados *TRUST-e*:

Teóricamente se ha argumentado que las páginas web tienen una "configuración de privacidad", que de conformidad con las garantías que ofrecen navegadores como Internet Explorer 6.0, serían "características de seguridad", y que se traducen muchas veces en *Certificados de Seguridad*. Estos Certificados pueden ser personales o de sitios web. Los primeros tienen que contener una declaración que compruebe la identidad de una persona o la seguridad de un sitio web. Se utilizan para comprobar la propia identidad del usuario y tiene en su equipo una clave privada que sólo éste conoce. Se los llama también "identificadores digitales". Los Certificados de sitios web tienen por objeto dar fe de que el sitio que se visita es seguro y genuino. Se asegura además que ningún otro sitio web puede suplantar la identidad del sitio seguro original. Sería útil a la hora de asegurarse que se protege la información de identidad personal que se envía.

Ambos tipos de certificados funcionan a través de una identidad o "clave pública". Sólo el propietario del certificado conoce la "clave privada correspondiente". Esta clave permite hacer una *firma digital* o decodificar información codificada con la clave pública correspondiente. Al enviar un mensaje a otra persona, en realidad se le daría la clave pública, de tal manera que se pueda recibir información que sólo el usuario puede descifrar y leer mediante su clave privada. Antes de iniciar el envío de información cifrado o firmado digitalmente, debe obtener un certificado y configurarlo a través de Internet. Cuando se remite un sitio web seguro (aquellos cuya dirección comienza con "https") el sitio le enviará automáticamente su certificado.

Muchos sitios web solicitan en la actualidad información de "Asistentes de Perfiles" donde la petición proporcionará: la dirección de Internet del sitio que solicita la información; toda información que se solicite al "Asistente de Perfiles"; cómo se utiliza esa información; si el sitio tiene conexión segura (o Secure Sockets Layer o SSL), que se comprueba a su vez con el respectivo certificado, etc...[344]

Otro sistema, que se asemeja bastante es el llamado *TRUSTe* que también es un sello o certificado de garantía que se otorgan a aquellos sitios web cuando éstos cumplen ciertos requisitos o políticas a favor de una adecuada protección a la intimidad de las personas. Según lo explica Javier Villate, habría tres tipos de sellos: en primer lugar, aquellos que garantizan que el sitio web no va a extraer ningún tipo de información personal; en segundo lugar, aquellos que se comprometen a no revelar datos de carácter personal ni de transferírselos a

[344] Esta información es la que ofrece el navegador de Microsoft, llamado Internet Explorer 6.0

terceros; y finalmente, aquellos que se reservan la facultad de revelar todo tipo de información a terceras partes. [345]

Muchos ven como necesidad primordial para que este tipo de sistemas de autorregulación funcionen un tremendo compromiso de buena fe por parte de las empresas que están detrás de esto. Sin embargo, no han tenido mucho éxito porque mucha gente está conciente que estas empresas no se mueven muchas veces por principios filantrópicos, sino por razones económicas...

4.- La Criptografía y la Firma Electrónica:

Este sistema, que fue implementado hace ya algunos siglos para permitir que mensajes ocultos fueran descifrados solamente por sus destinatarios ha tenido gran uso a nivel militar, y en la actualidad es una de las latentes soluciones al momento de buscar intimidad en el ciberespacio. Se dice que la palabra criptología proviene de las palabras griegas Kryto y logos y siginifica "estudio de lo oculto". Una rama de la criptología es la criptografía, que se ocupa del cifrado de mensajes. Ésta se basa en que el emisor emite un mensaje en claro, que es tratado mediante un cifrador con la ayuda de una clave, para crear un texto cifrado. Este texto cifrado, por medio del canal de comunicación establecido, llega al descifrador que convierte el texto cifrado, apoyándose en otra clave, para obtener el texto en claro original. [346]

De esta manera, lo que se propone es crear una clave que permita que el usuario no sea identificado en la red, y que por consiguiente, pueda navegar con la tranquilidad de que las huellas que va dejando no lo individualicen. Se han propuesto programas como el PGP, que permiten cifrar, descifrar y firmar digitalmente de forma segura (aparentemente), las comunicaciones de los usuarios. Se obtiene de forma gratuita y se puede instalar en los computadores bajando el programa a través de Internet.

Sin embargo, esta solución también a encontrado detractores, que argumentan que "esta alternativa que a primera vista parece la más adecuada y fácil ofrece problemas. El primero es que seguramente los que comercian con la información serán los primeros interesados en vender ese software a precios poco accesibles lo cual degenerará en unos pocos afortunados que puedan pagar por su privacidad. Si lo ofreciesen gratuitamente podrían pedir igualmente nuestros nombres para la licencia de uso (lo cual ocurre en cualquier utilitario al cual hagamos un download)." [347]

---

[345] Javier VILLATE, P3P, un estándar para la privacidad. ¿Es lo que necesitamos?, pág. 3 de texto publicado en http://vlex.com/redi/No._01_-_Agosto_de_1998/villate, visitado en diciembre de 2001. Para tener más información sobre este sistema TRUSTe, remitirse a http://www.truste.org.

[346] Esta información se obtuvo de la página web de la Asociación de Internautas, y el texto se puede obtener directamente en http://seguridad.internautas.org/criptografia.php, visitado en abril del 2002. Para obtener mayor información acerca de la criptografía, se recomienda visitar el sitio web www.kriptopolis.com .

[347] Amílcar MENDOZA LUNA, Perú: Los Cookies ¿amenaza a la privacidad de información en la internet?, pág. 6 de texto publicado en http://vlex.com/redi/No._30_-_Enero_del_2001/8, visitado en enero de 2002. Aprovecho para explicar el significado de las siguientes palabras: Se define a *software* (programas, componentes lógicos, *software*) como "Programas o elementos lógicos que hacen funcionar un ordenador o una red, o que se ejecutan en ellos, en

En Chile se acaba de promulgar una ley que reconoce el uso de la firma electrónica (ver en el capítulo tercero comentarios al respecto), y de la que se espera, tenga gran aplicación en la sociedad. Sin embargo, es difícil creer que la utilización de la criptografía pueda ser una solución al largo plazo, ya que así como se crean programas increíbles para inventar claves aparentemente inviolables, de la misma manera irán apareciendo nuevos programas que vayan resolviendo estas combinaciones de seguridad, y que de seguro se irán comercializando y popularizando en la misma red.

5.- Programas filtro:

Como su nombre bien lo indica, se trata de programas que tienen por objeto filtrar aquellos contenidos que sean ilícitos o no deseados por el usuario mientras éste transita en el ciberespacio. La descripción de estos programas, según explicación de Jijena Leiva, es la siguiente:

"Existen tres tipos esenciales de programas filtro: los de lista negra, que bloquean el acceso a determinados emplazamientos; los de lista blanca, que permiten el acceso a determinados sitios WEB autorizados expresamente y bloquean los restantes; y los de etiqueta neutra, que asignan una etiqueta o valoración a los sitios y permiten que el usuario final decida su uso, clasifique o seleccione los contenidos y bloquee los que desee (son los filtros PICS -Plataform for Internet Content Selection- o Plataformas para la Selección de Contenidos en Internet). Entre los usuarios de la red a estos software se les llama "Net Nanny" o "niñeras para la red" y son de fácil adquisición en el mercado. (...) Se trata de un nivel de censura o más bien de autocensura totalmente aceptable que, pragmáticamente, permite respetar la diferencia de criterios, valores o costumbres morales entre comunidades, países y culturas diversas. Ya no hay eventual censura en la fuente o alguna restricción o prohibición legal, administrativa o judicial previa para publicar virtualmente determinados contenidos, sino que el control o filtrado se produce a nivel de usuario final en el computador donde se recibe la información."[348]

Según palabras del mismo autor, "Si los usuarios pueden contar con programas que les permiten filtrar los contenidos, se hace plenamente factible permitir la libre circulación de la información reclamada por la libertad de expresión y el respeto a las preferencias personales, por ejemplo de los padres que quieran controlar el material a que acceden sus hijos." [349]

---

contraposición con los componentes físicos del ordenador o la red"; y *download* (descargar, *bajar* ,bajarse) "En Internet proceso de transferir información desde un servidor de información al propio ordenador personal." Definiciones obtenidas de Glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitada en marzo del 2002.

[348] Renato JIJENA LEIVA, en Responsabilidad de los ISP por la difusión de contenidos on line, pág. 5.

[349] Ibídem.

Soluciones jurídicas

1.- Los Códigos de Conducta:

Estos códigos, llamados también "Códigos Deontológicos", han sido aplicados en distintos ordenamientos jurídicos europeos, de lo cual se puede dar fe en el segundo capítulo de este trabajo. De hecho, la propia Directiva 95/46/CE los ha considerado como una solución factible, promoviendo en su artículo 27 "la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva"[350]

La profesora española Ana Isabel Herrán Ortiz los define como "normas de autorregulación de los diferentes sectores en el ámbito de la protección de datos personales. Estas prácticas se contemplan con interés desde los Estados, ya que constituyen una forma de alcanzar la protección de datos desde la buena voluntad de los sectores empresariales implicados en los tratamientos de datos personales, no en vano se trata de normas de autorregulación de los tratamientos de datos personales."[351] Como lo señala la mencionada autora, éstos códigos no son ajenos a las autoridades de control de los países, por lo cual deben ajustarse a las exigencias que dichas autoridades establezcan, y que en definitiva se ajusten en el caso europeo, a las prescripciones comunitarias.

Cabe resaltar que no existen solamente códigos de conducta nacionales, sino que también están los códigos de conducta comunitarios, y que se hallan sometidos al control del Grupo de Protección de Personas como órgano de tutela de la Unión Europea. Este Grupo tiene por objeto velar para que tales códigos se adapten a las exigencias de las normas nacionales sobre protección de datos.

Pero como lo señala la propia Herrán Ortiz, "Ha merecido importantes críticas para la doctrina la regulación de los códigos de conducta en la Directiva europea, porque se afirma que con dicha regulación, excesivamente flexible, se facilita la aprobación de disposiciones reglamentarias sectoriales, que abandonan al criterio de cada Estado la opción sobre el desarrollo normativo de estos códigos ."[352]

2.- La Autorregulación de la red:

Muchos han argumentado que, por las características de Internet, encontrar un conjunto de normas que permita solucionar los inconvenientes que se presentan en el ciberespacio es imposible. De esta manera, en los inicios de este nuevo medio de comunicación, la autorregulación fue la opción por la cual optaron

[350] Extracto del Artículo 27 de la Directiva 95/46/CE de la Unión Europea.

[351] Ana Isabel HERRÁN ORTIZ, España: La protección de datos personales en el marco de la Unión Europea, pág. 21 de texto publicado en http://vlex.com/redi/No._39_-_Octubre_del_2001/6, visitado en enero de 2002.

[352] Ibídem, pág. 22.

prácticamente todos quienes intervenían en el ciberespacio. Aún cuando algunas de las soluciones anteriormente presentadas se aplican a través de la autorregulación, hemos creído que es preciso analizarla como solución propiamente tal.

En la actualidad, todavía existen muchos partidarios de este método a la hora de regular la red. Bill Gates es uno de ellos, quien ha manifestado que: "Los efectos económicos de Internet son resultado de la libertad que impera en la red, por lo que cualquier regulación tendrá un precio: perder crecimiento económico.(...). En los próximos años, la gente aumentará su confianza en Internet para compartir información delicada con interlocutores confiables acerca de sus finanzas, historias médicas, hábitos personales o preferencias como compradores. Al mismo tiempo, muchos pueden querer mantener en reserva esta información y usar Internet en forma anónima(...). Esto ha dejado a mucha gente renuente a proporcionar datos reales a sitios Web. La industria privada y muchas herramientas de autorregulación del gobierno, así como determinadas tecnologías, son la mejor forma de proteger la privacidad."[353] (subrayado es mío).

Dentro de la doctrina chilena, Jijena Leiva también considera que la autorregulación es una buena solución, argumentando que: "Deben por ende considerarse como una opción jurídica viable las modalidades de autoregulación. Por su propio peso e importancia el desarrollo y los conflictos jurídicos en Internet pueden traducirse en el surgimiento de normativas que, impulsadas por algún país u organismo internacional, tengan acogida y sean aceptadas mundialmente por los usuarios de la red. Así ha ocurrido con la reglamentación desarrollada por la IANA[354] y la ICANN[355] en relación a la asignación de direcciones virtuales o de los nombres de dominio."[356]

Sin embrago, la autorregulación parece en todo caso haber encontrado más opositores que partidarios. Uno de ellos es David Casacuberta, quien desde mi punto de vista en una forma clara y precisa ha señalado que: "En primer lugar está el problema de que toda norma ética adoptada unilateralmente, por buena voluntad, puede también disolverse unilateralmente, sin que el cliente tenga la menor posibilidad de protestar, no quedándole más remedio que emular a Job y musitar "El Mercado lo dio, el Mercado lo quitó".

Las razones que pueden llevar a un cambio así son múltiples: la empresa en cuestión aunque actúa de buena fe, es absorbida por otra que no respeta la privacidad, de forma que todos los acuerdos anteriores no son válidos; la empresa no se caracteriza por su buena fe y un día decide cambiar el rumbo de su negocio y

---

[353] William H. GATES, Ensayo para el Presidente de Estados Unidos, texto publicado de www.emol.cl con fecha 8 de febrero de 2001, visitado por el autor de este trabajo en la misma fecha.

[354] La sigla corresponde a la *Internet Assigned Numbers Authority*, un organismo contratado por el Gobierno de EE.UU. para administrar técnicamente el sistema de direcciones o nombres de dominio en la red.(nota de Renato JIJENA LEIVA)

[355] La sigla corresponde a la *Internet Corporation for Assigned Names and Numbers*, (nota de Renato JIJENA LEIVA).

[356] Renato JIJENA LEIVA, en Responsabilidad de los ISP por la difusión de contenidos on line, pág. 18. Quiero hacer un comentario respecto de este párrafo del profesor Jijena, y es que la IANA ya no existe y fue reemplazada por la ICAAN. Por consiguiente, no debe considerarse como dos organismos distintos cuando el realidad son el mismo, pero con distinto nombre.

dedicarse a la venta de datos personales; la empresa tiene buena fe pero no quiere problemas y ofrece datos personales a la policía o a una empresa más grande sin preocuparse de respetar su criterio y sin tener una orden judicial... Lo peor de todo es que hay ejemplos de todos y cada uno de estos casos, así que no estamos haciendo ciberderechos-ficción.

En segundo lugar, si nos hemos de guiar por los ejemplos actuales, la "autoregulación empresarial" no es más que una colección de tópicos uno detrás de otro, y las afirmaciones son demasiado generales para constituir ninguna garantía real. Sin una normativa muy específica detrás que permita al usuario consultar la base de datos y ver qué tiene la empresa sobre él, saber qué sucede con los datos si la empresa es comprada o absorbida por otra, o conocer si hay cookies, donde se almacenan y qué tipo de perfiles se genera de cada usuario, una pomposa declaración del tipo "En la empresa XYZ se respeta su privacidad" es equivalente a decir "Si utiliza los servicios telemáticos de la empresa XYZ las mujeres lo encontrarán irresistible". Un mero gancho publicitario.

En tercer lugar, la tentación es demasiado grande como para confiar en la autorregulación. Stephen Lau, de la Comisión para la privacidad de datos personales en Hong-Kong, durante una mesa redonda, capturó de forma excelente este punto, al indicar que confiar en la autorregulación empresarial en el tema de la privacidad es como esperar que Drácula se porte bien en un banco de sangre. Hay demasiados beneficios en juego.

En un plano más teórico, observemos que todo sistema de autorregulación empresarial está en contra de la idea de justicia distributiva, pues plantea una discriminación por status socio-económico. Como hemos dicho ya varias veces, vender datos personales es uno de los negocios más redondos de Internet. Las empresas que decidan no entrar en ese negocio necesitarán una compensación, siguiendo las leyes del mercado. El resultado final nos llevará a que la privacidad sea un producto en venta, y seguramente un producto caro. Sólo las personas con un mayor poder adquisitivo podrán permitirse pagar su privacidad. El resto se verá obligado a utilizar conexiones baratas en las que sus datos personales estarán en las bases de datos de medio mundo."[357]

Soy bastante partidario de la postura de Casacuberta, ya que como bien lo argumenta este autor, es muy probable que los intereses económicos puedan más que la buena fe por defender un derecho fundamental. Eso hace que las reglas del juego puedan cambiarse según los intereses del mercado, y es verdad que los bancos datos de carácter personal son muy cotizados en el ciberespacio. Insisto en las palabras de Stephen Lau, la tentación es demasiado grande...sobre todo en una sociedad como la nuestra donde el proverbio de que *información es poder* cobra más fuerza cada día.

---

[357] David CASACUBERTA, La privacidad en los nuevos medios electrónicos, de texto publicado en http://v2.vlex.com/global/redi/redi_numero.asp?numero=%2311&fecha=Junio+1999, pág. 4, visitada en diciembre de 2001. Ver también a este respecto las opiniones de Amílcar MENDOZA LUNA en Perú: Los cookies ¿amenaza a la privacidad de información en la internet?, pág. 13 de texto publicado en http://vlex.com/redi/No._30_-_Enero_del_2001/8, visitado en enero del 2002; y de Argido GERALDO QUINTERO, en Colombia: El Secreto en la Comunicación por Correo Electrónico, págs. 10 y 11 de texto publicado en http://publicaciones.derecho.org/redi/No._25_-_Agosto_del_2000/3, visitado en enero de 2002.

Pero, para Casacuberta la solución a la privacidad pasa por tres vías complementarias: la existencia de leyes protectoras de la privacidad, las tecnologías informáticas que permitan el anonimato y la toma de conciencia por parte de los ciudadanos.

3.- Los Programas *Safe Harbor*:

Esta es una solución que también ha sido adoptada por la Directiva de la Unión Europea, que ha exigido a los países miembros la condición de que sólo pueden ser transferidos los datos de carácter personal de sus ciudadanos siempre y cuando el país de destino ofrezca garantías suficientes y equivalentes a las que ofrece el país remitente: es decir, se busca que dicha información llegue a "puerto seguro".[358] Tiene sus antecedentes en políticas promovidas por el Convenio del Consejo de Europa en su artículo 12 (y que consiste básicamente en que un Estado no debe imponer restricciones a la exportación de datos personales a otro Estado que les acuerde una protección sustancialmente equivalente a la que reciben en el país exportador); las recomendaciones de la OCDE que establecía en su artículo 17 el "principio de la equivalencia", más tarde recogidas por la ONU, y que en realidad se han traducido en "buscar un equilibrio entre la protección del derecho a la vida privada y los intereses legítimos, públicos y privados que pueden obtenerse de su tratamiento informatizado".[359]

Esta política fue puesta en marcha justamente entre los europeos y los norteamericanos, estos últimos carentes de una normativa suficientemente segura en cuanto al tratamiento de datos de carácter personal a nivel internacional. Así, el Grupo de los Quince habría permitido que se transfieran datos de carácter personal a empresas u organizaciones que, a través de una autodeclaración o autocertificación de la propia entidad, se adapta a las exigencias del Departamento de Comercio de la Unión Europea. Esta fue una puerta de salida por ejemplo para las multinacionales, que al estar establecidas en Europa, se supone que no podían trasmitir este tipo de datos a los Estados Unidos.

Sin embargo, con la llegada de Internet, muchos cuestionan que este sistema Safe Harbor pueda funcionar a cabalidad. De ello se desprende que aún cuando existan compromisos entre países para proteger la transmisión de datos de carácter personal, no existe certeza absoluta de que efectivamente información nuestra llegue a puerto seguro.

---

[358] Según el artículo 25 de la Directiva de la Unión Europea, transferir los datos hacia países con unas salvaguardas menos rigurosas supone una violación de la norma comunitaria, y más concretamente de las legislaciones nacionales, y es, por tanto, susceptible, de sanción. De esta manera, se ordena a la Comisión que negocie con aquellos países que no estén a la altura de la protección europea y la habilita para, en su caso, a la vista de la legislación interna y los compromisos internacionales, certificar la adecuación al standard del Estado en cuestión .

[359] Rafael DÍAZ ARIAS, en España: Transferencia de Datos Personales. ¿Llegarán nuestros datos a buen puerto?, sobre el reciente acuerdo sobre protección de datos alcanzado entre Estados Unidos y la Unión Europea, pág. 2 de texto publicado en http://publicaciones.derecho.org/redi/No._23_-_Junio_del_2000/8, visitado en diciembre de 2001. Para ver con más detalle los textos de los organismos citados, remitirse a la obra de Mercedes URIOSTE, Protección de Datos Personales, de Revista de la Secretaría de Derecho Comparado de la Corte Suprema de la Nación Argentina, pág.5,de texto publicado en http://comunidad.derecho.org/redi/Habeas6.zip, visitado en enero de 2002. Este texto será citado frecuentemente porque es una fuente muy completa de información.

4.-La Creación de un Organismo Internacional:

Se trata de un proyecto que pretende, a través de acuerdos o convenios internacionales, crear una Autoridad que tenga reconocimiento a nivel mundial y ante la cual se pueda acudir en el caso de que se cometan atentados como el violar el derecho a la intimidad de las personas a través de la red. Este organismo, al igual que la directiva de la ONU, estaría integrado por miembros de varios países del mundo. Según el autor de este trabajo, esta solución no es una alternativa utópica, ya que si bien Internet se caracteriza por no tener un gobierno determinado y ser a-territorial, podría tratarse de un organismo que establezca cuales son las directrices por las que los internautas deben guiarse al navegar en la red. De la misma manera que existen organismos internacionales que se encargan de velar por el cumplimiento y la no violación de derechos humanos, esta entidad podría adquirir la calidad de Tribunal Internacional frente a los abusos que se cometen en Internet. De él podría por ejemplo emanar una "ciberpolicía", entidad encargada de combatir los ilícitos que se susciten en la red.

Esta solución ha sido ya considerada en algunos países, y de hecho en la actualidad existe un proyecto llamado GIC, cuyas siglas son *Group of Internationalization of Internet* y que pretende se vaya cuajando a nivel internacional.

Al igual que como funcionan Tratados como el Pacto de San José de Costa Rica, la idea es que los ordenamientos jurídicos internos de cada país dictes sus propias normas respetando siempre las directrices que este Tratado Internacional llegara a imponer. De hecho, aún cuando este principio ya ha tenido éxito en la Unión Europea a través de las bases que ha ido dictando su propia Directiva, sería prudente que si se crea este organismo internacional, se transforme a grandes rasgos en una "Directiva", pero a nivel mundial.

Y es que efectivamente, parece inútil que cada Estado dicte sus propias normas respecto a Internet, si para violarlas basta con cambiarse a otro territorio jurisdiccional donde éstas sean inexistentes o más flexibles. En la actualidad no existen principios claramente establecidos que tengan aceptación a nivel mundial, y cometer delitos a través de la red es tan fácil como quitarle el caramelo a un niño.

Los detractores de esta postura van a defender el hecho de que Internet no puede dejar de ser un espacio virtual y por naturaleza libre. Pero lo que ellos no han recordado es que la libertad absoluta no existe, ya que el límite de ésta se encuentra en el respeto de los derechos que por esencia son propios del hombre, y por consiguiente no puede bajo ningún punto de vista permitirse que exista una herramienta para que éstos puedan ser amenazados o violados.

5.- Aplicación del Teorema de *Coase*:

Hay quienes creen que, aplicando el Teorema del Premio Nobel de Economía Ronald Coase, los ilícitos que se dan en la red pueden encontrar una salida. Según la explicación de Craig R. Giesze[360], "toda negociación requiere tiempo y energía, y cuando los beneficios potenciales son pequeños, puede darse el caso de que no merezca la pena.(...)". Refiriéndose al Teorema propiamente tal, Giesze agrega que: "la versión *positiva* del Teorema de Coase establece que los litigantes involucrados en un conflicto sobre los derechos de propiedad pueden negociar entre ellos la solución más eficiente –al evitar el aparato legal y judicial- siempre y cuando existan dos condiciones claves: 1) que los costos de transacción de las negociacions privadas sean cero; y 2) que la asignación de los derechos, obligaciones y responsabilidades de las partes sea bien delimitada[361]. (...) Alternativamente, la aplicación *normativa* del Teorema de Coase dispone que si los costos de transacción de las negociaciones privadas son altos o prohibitivos (por ejemplo, muchas partes involucradas), o si los derechos, obligaciones y responsabilidades legales entre los particulares son mal especificados, entonces el Estado debe intervenir para "lubricar" el proceso de negociación entre ellos. En este contexto, el Estado debe promulgar una ley o una norma jurídica cuyo efecto es reducir los costos de transacción de las negociaciones privadas o aclarar la asignación de los derechos, obligaciones y responsabilidades legales entre las partes, con la finalidad de facilitar el proceso negociador. Así, la aplicación normativa del Teorema de Coase puede fomentar la adopción de transacciones extrajudiciales eficientes entre los particulares[362]".

Si analizamos con cuidado este Teorema podremos ver que existe un "único contaminador" que en este caso específico es Internet, ya que a través de este medio de comunicación es que se cometen los ilícitos. Debe además tomarse en cuenta que los datos de carácter personal de una persona pueden considerarse como un bien propio de ésta, ya que por esencia le pertenecen y puede disponer de ellos, por ejemplo, comercializándolos.

Aplicando este Teorema al caso específico de la protección del derecho a la vida privada de las personas en Internet, más específicamente a sus datos de carácter personal, podemos llegar a las siguientes conclusiones:1) los costos de transacción de las negociaciones entre privados van a ser altos definitivamente; 2) los derechos, obligaciones y responsabilidades legales entre quienes participan en la red no están muy definidos, además de que son bastante complejos y únicos; 3) existen muchas personas desconocidas involucradas en las negociaciones;4) el ambiente para negociar no es precisamente el más favorable;5) hay

[360] Craig R. GIESZE, El análisis económico de la información privilegiada en el mercado de capitales y valores: ¿justicia ineficiente?, de texto publicado en Revista Chilena de Derecho, Vol. 26 N°4, 1999, pág 823.

[361] Los costos de transacción de las negociaciones entre los privados son normalmente muy bajos, y la asignación de los derechos, obligaciones y responsabilidades de las partes es usualmente bien delimitada en las siguientes circunstancias: 1) bienes y servicios estandarizados; 2) derechos muy específicos; 3) pocas personas desconocidas involucradas en las negociaciones; 4) buen ambiente negociador; 5)conocimiento entre los negociadores; 6) comportamiento razonable; 7) intercambios inmediatos; 8) contingencias; 9) bajo costo de monitoreo; y 10) castigos de bajo costo.

[362] En términos generales, los costos de transacción de las negociaciones privadas son altos o prohibitivos y, en su caso, los derechos, obligaciones y responsabilidades legales de las partes son mal especificados en las siguientes circunstancias: 1) bienes y servicios únicos; 2) derechos complejos o múltiples; 3) muchas personas desconocidas involucradas en las negociaciones; 4) mal ambiente negociador; 5) poco conocimiento entre los negociadores; 6) comportamiento irracional; 7) intercambios a lo largo de tiempo; 8)falta de contingencias; 9) alto costo de monitoreo; y 10) castigos de alto costo.

poco conocimiento entre los negociadores;6) un comportamiento irracional no sería de extrañar;7) de producirse un intercambio, no parece que éste sea de corto plazo;8) no hay contingencias; 9) se daría un alto costo de monitoreo y; 10) se ha demostrado que los castigos son de alto costo.

Por lo anteriormente expuesto se puede deducir que de aplicarse este Teorema, debe hacerse en su versión *normativa.* Como consecuencia de ello, las medidas a tomar por parte de un Estado, por ejemplo el chileno, serían las siguientes:

1) Promulgar una ley o una norma jurídica que tenga por objeto hacer que los costos de transacción entre las partes disminuyan, ello por ejemplo a través de la creación de un órgano encargado de juntar a las partes afectadas y de hacer que su actuación se realice conjuntamente y no por separado. De esta manera, el costo que se invertiría en un proceso judicial individual se reduciría de manera considerable si éste se hace en conjunto, constituyendo un importante incentivo para quienes vean, en este caso concreto, su derecho a la intimidad afectado.

2) Aclarar la asignación de los derechos, obligaciones y responsabilidades de quienes son sujetos activos pasivos en el uso de Internet, determinando así el rol que cada uno de ellos tiene.

Aproximarse a dar una solución específica de cómo solucionar la protección del derecho a la vida privada de las personas me parece un proyecto bastante apresurado y ambicioso. Si analizamos el caso chileno en espacial, creo que hay muchas cosas que hacer en el camino. Una de ellas es modificar la ley 19.628, de tal manera que se adapte a las exigencias internacionales que otros ordenamientos como los europeos han establecido en este sentido. Chile no puede considerarse este momento como un "puerto seguro" para quienes pretendan llevar a cabo una transferencia de datos desde un país que sí cumpla con estas políticas.

Además, en Chile no existe una Agencia de Protección de Datos, por lo cual en caso de que se cometan abusos que puedan afectar la intimidad de las personas, el acudir a los tribunales de justicia puede verse en la gran mayoría de los casos como insuficiente. En varios países europeos y en otros latinoamericanos como Argentina, el actuar de este tipo de organismos ha demostrado ser un arma que permite combatir este tipo de arbitrariedades.

La Constitución de la República de Chile es especialmente clara y cuidadosa en señalar en su artículo primero, inciso cuarto, que:

"El Estado está al servicio de la persona humana y su finalidad es promover el bien común, para lo cual debe contribuir a crear las condiciones sociales que permitan a todos y cada uno de los integrantes de la

comunidad nacional su mayor realización espiritual y material posible, con pleno respeto a los derechos y Garantías que esta Constitución establece". [363]

Por ello, es deber del Estado velar porque sus miembros gocen y ejerzan derechos como el de tener una vida privada, indispensable para alcanzar un desarrollo tanto material como espiritual, y fundamental a la hora de buscar promover el bien común entre los hombres.

A causa de ello, cada día se vuelve más imperiosa la necesidad de legislar acerca del manejo y uso de Internet, y eso se ha visto reflejado tanto en las recientes normas que han sido promulgadas en los ordenamientos jurídicos de países de casi todo el mundo, como en la abundante cantidad de proyectos de ley que se discuten día a día en los parlamentos. Esto quiere decir que el legislador está tomando conciencia que estamos frente a una poderosa herramienta que merece ser cuidadosamente regulada. Al momento de legislar, creo indispensable la participación de expertos de distintos rubros en el tema, ya que seamos realistas, una gran cantidad de quienes estamos involucrados en el mundo de las leyes no tenemos ni la más remota idea de cómo funcionan las nuevas tecnologías ni de cómo éstas pueden llegar a alcanzar una solución coherente.

Considero así mismo que, sea cual fuere la postura que se adopte, es indispensable que en ella exista una perfecta armonía entre el derecho y la tecnología, sin que se desconozca bajo ningún punto de vista la participación de esta última al momento de buscar una solución.

Finalmente, quiero puntualizar que detrás de esto tiene que haber un esfuerzo por parte de varios sectores de la sociedad, y ello trae consigo una enorme tarea de toma de conciencia y educación respecto de todas las grandes ventajas que las nuevas tecnologías están haciendo día a día en un nuestra vida cotidiana, y de las desventajas que éstas también acarrean consigo. La tarea es grande y el camino es largo.

[363] Artículo primero, inciso cuarto de la Constitución de la República de Chile.

CONCLUSIÓN

El derecho a la vida privada que tenemos todas las personas es un derecho que por su naturaleza se encuentra en constante evolución. Eso hace que se vuelva extremadamente complicado encontrar una definición que se adapte en el tiempo y en el espacio. Por ello, al tratar de determinar el alcance que debe tener este derecho, ya la Comisión de Estudio de la Nueva Constitución, a través de la figura de don Jaime Guzmán Errázuriz señalaba que: "*En cuanto a que se fije por la jurisprudencia los límites, le parece que va a ser inevitable que así sea. No cree que la Constitución pueda, al tratar de los medios de comunicación, ser demasiado precisa en cuanto hasta dónde se extienda el ámbito de la privacidad, porque es evidente, por ejemplo, que la persona que actúa en la vida pública debe entender, en su opinión, que cierta parte de su vida privada está en tela de juicio en una mayor medida que la de una persona que jamás ha intentado actuar en la vida pública (...)*"[364]. Dentro de lo que comprende la vida privada de las personas, ha nacido a la vida del derecho la necesidad de proteger el tratamiento, uso y transferencia de los datos personales de las personas. Distintos Tratados Internacionales y ordenamientos jurídicos de varios países han salido al paso de este desafío.

Chile no ha sido la excepción y, reconociendo junto con otras normas, dentro de su sistema legal la protección del derecho a la vida privada de las personas a través de nuevas acciones como la de *Habeas Data* (cuya aplicación es escasísima, por no decir nula), ha pretendido ponerse a la altura del derecho comparado. Sin embargo, aún cuando los esfuerzos han sido significativos, están lejos de ser suficientes, sobre todo, con la llegada de nuevas tecnologías como Internet.

Al entrar en la era de la llamada *Sociedad de la Información*, el mundo ha dado los primeros pasos hacia una nueva generación, donde las modernas tecnologías que se utilizan para las telecomunicaciones han sido la principal amenaza a la hora de proteger la vida íntima de las personas. *Información es poder*, y ahora más que nunca, existe un interés superior por conocer aspectos de nuestra vida. A diferencia de otras épocas donde los motivos por conocer nuestra intimidad estaban relacionados con fines militares o publicitarios, en la actualidad existen otras intenciones, motivadas más por revelar todo un comportamiento que permita hacer de cada uno de nosotros verdaderos perfiles con un grado de exactitud sorprendente. Detrás de esto está un

[364] Discurso pronunciado por don Juan GUZMÁN ERRÁZURIZ, durante la sesión n° 129 celebrada el 12 de junio de 1975 por la Comisión de Estudio de la Nueva Constitución. Citado por el profesor don José Luis CEA EGAÑA en Manual de Derecho Constitucional, Tomo II, referente a los Derechos, Deberes y Garantías Constitucionales, pág. 90, texto de estudio para la Pontificia Universidad católica de Chile, 1996.

interés económico, en un mundo donde bancos de datos personales se han transformado en un bien preciado. Con la llegada de Internet, las posibilidades tanto de explorar datos y hechos de nuestra esfera íntima como de transmitirlos se transformó en una práctica para muchos, y lo peor de todo, sin que siquiera nos percatáramos de ello. Los nuevos medios de comunicación y en especial Internet, son la principal herramienta de este comercio de información, y al ser un negocio, el debido resguardo de esta garantía fundamental tiene por delante una traba que muchas veces se vuelve difícil de sobrepasar.

Comparto con aquellos que creen que la tecnología no trae solamente cosas malas, y estoy conciente de que Internet ha revolucionado la manera de vivir de las personas, pero soy partidario de que todo avance científico vaya de la mano de un delicadísimo proceso de adaptación de las nuevas tecnologías con lo que, por esencia, le pertenece al hombre en su condición de tal: sus principios, sus deberes y sus derechos. Y justamente, al existir en la actualidad toda una amenaza frente a derechos de la más alta jerarquía como el derecho a la vida privada, es menester que los Estados tomen cartas en el asunto.

Creo que la solución no se encuentra en un manual de derecho ni en otro de tecnología. Desde mi punto de vista, la respuesta está en un trabajo armonioso entre los distintos grupos que conforman una sociedad, donde deben ser considerados aspectos tanto técnicos como jurídicos, y donde la labor de educar a sus miembros es tarea fundamental. Sin duda alguna que se vuelve necesario crear nuevas leyes y perfeccionar las existentes para resguardar más a cabalidad la vida íntima de las personas y de esta manera alcanzar el bien común en una sociedad que aspire principios democráticos y pluralistas.

He querido retomar la idea del francés Pierre Kayser, donde el *respeto* y la *libertad* de la vida privada de las personas deben encontrarse correspondidos por una libertad de pensamiento y de sentimientos que no pueden ser destruidos, ni siquiera por la Autoridad. Recordemos que detrás de nuestra esfera íntima, está también una familia, una imagen y un honor que merecen ser protegidos como el más preciado tesoro. Conciente de que la vida útil de parte de este trabajo puede ser corta debido a los constantes desarrollos de la ciencia, no me queda más que decir que la vida privada de las personas también está destinada a desarrollarse y a resguardarse, y es deber del Estado sentar las bases para ello.

BIBLIOGRAFÍA

1.- BARRERA María Helena, "Correspondencia Digital: Recreando Privacidad en el Ciberespacio", en Revista Electrónica de Derecho Informático N° 15 de octubre de 1999, cuyo texto se encuentra publicado en http://www.digital-law.net/IJCLP/3_1999/ijclp_webdoc_4_3_1999.html de International Journal of Communications Law and Policy, Summer 1999, Oxford University.

2.- CARRASCO BLANC Humberto, "Chile: Algunos Aspectos de la Responsabilidad de los Proveedores de Servicio y Contenidos de Internet. El caso ENTEL", en Revista Electrónica de Derecho Informátcio N° 26 de septiembre de 2000, cuyo texto se encuentra publicado en http://vlex.com/redi/No._26_-_Septiembre_del_2000/4

3.- CASACUBERTA David, "La privacidad en los nuevos medios electrónicos", en Revista Electrónica de Derecho Informático N° 11, cuyo texto se encuentra en http://v2.vlex.com/global/redi/redi_numero.asp?numero=%2311&fecha=Junio+1999

4.- CASTILLO MARCANO José Luis, "El Derecho a la Intimidad y la Protección de Datos Personales en el Derecho Español", En Boletín de la Academia de Ciencias Políticas y Sociales. Nº 134. Año LXIV, Caracas, 1997.

5.- CEA EGAÑA José Luis, "Manual de Derecho Constitucional", Tomo II, 1996.

6.- CEA EGAÑA José Luis, "Vida pública, vida privada y derecho a la información: acerca del secreto de reserva", Revista de Derecho, Facultad de Ciencias Jurídicas y Sociales, Universidad Austral, Vol. III, N° 1-2, diciembre de 1992.

7.- Contratos que ENTEL Chile S.A. ofrece a sus clientes para acceder a Internet.

8.- CORRAL TALCIANI Hernán Configuración Jurídica del Derecho a la Privacidad I, de texto publicado en Revista Chilena de Derecho, Vol. 27 N°1, Sección Estudios.

9.- CORRAL TALCIANI Hernán Configuración Jurídica del Derecho a la Privacidad II, de texto publicado en Revista Chilena de Derecho, Vol. 27 N°2, Sección Estudios.

10.- CUERVO José, "La intimidad informática del trabajador", en Revista Electrónica de Derecho Informático N° 3 de octubre de 1998, cuyo texto se encuentra en http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=106971

11.- Del Archivo de Gaceta Jurídica, N° 239, Recurso de Protección N° 243-1999 contra ENTEL Chile S.A., edición de Mayo del 2000, Santiago, Chile.

12.- DÍAZ ARIAS Rafael, "España: Transferencia de Datos Personales. ¿Llegarán nuestros datos a buen puerto?, sobre el reciente acuerdo sobre protección de datos alcanzado entre Estados Unidos y la Unión Europea", en Revista Electrónica de Derecho Informático N° 23 de junio de 2000, cuyo texto se encuentra publicado en http://publicaciones.derecho.org/redi/No._23_-_Junio_del_2000/8

13.- Diccionario de la Lengua Española, Real Academia Española, Vigésima Primera Edición, Madrid.

14.- ELIAS Miguel S., "Argentina: Situación Legal de los Datos de Carácter Personal frente a las Nuevas Tecnologías", en Revista Electrónica de Derecho Informático N° 32 de marzo de 200, cuyo texto se encuentra publicado en http://vlex.com/redi/No._32_-_Marzo_del_2001/10

15.- EVANS DE LA CUADRA Enrique, "Los Derechos Constitucionales", Tomo I, Editorial Jurídica de Chile, Santiago de Chile, 1986.

16.- FERNÁNDEZ GONZÁLEZ Miguel Ángel, "Libertad de expresión, censura previa y protección, en Revista Chilena de Derecho, Vol. 28, año 2001.

17.- FROSINI Vittorio, "Informática y Derecho", Editorial Temis S.A., Santa fe de Bogotá, Colombia, 1988.

18.- GARCÍA ASPILLAGA Raúl, "La vida privada y la intimidad de las personas", Tesis de Grado de la Facultad de Derecho de la Pontificia Universidad Católica de Chile,1988.

19.- GATES William H., "Ensayo para el Presidente de Estados Unidos",cuyo texto se encuentra publicado en www.emol.cl con fecha 8 de febrero de 2001.

20.- GERALDO QUINTERO Argido, "Colombia: El Secreto en la Comunicación por Correo Electrónico", en Revista Electrónica de Derecho Informático N° 25 de agosto del 2000, cuyo texto se encuentra publicado en http://publicaciones.derecho.org/redi/No._25_-_Agosto_del_2000/3

21.- GIESZE Craig R., "El análisis económico de la información privilegiada en el mercado de capitales y valores: ¿justicia ineficiente?", de texto publicado en Revista Chilena de Derecho, Vol. 26 N°4, 1999, pág 811.

22.- HERRÁN ORTIZ Ana Isabel, "España: La protección de datos personales en el marco de la Unión Europea", en Revista Electrónica de Derecho Informático N° 39 de octubre de 2001, cuyo texto se encuentra publicado en http://vlex.com/redi/No._39_-_Octubre_del_2001/6

23.- HERRÁN ORTIZ Ana Isabel, "La violación de la intimidad en la protección de datos personales", Editorial Dykinson, Madrid, 1998.

24.- HERRERA BRAVO Rodolfo, "Chile, España: La Legitimidad del Control Tecnológico del Empleador sobre el Trabajador", en Revista Electrónica de Derecho Informático N° 35 de junio de 2001, cuyo texto se encuentra publicado en http://vlex.com/redi/No._35_-_Junio_del_2001/4

25.- HERRERA BRAVO Rodolfo, "Chile: ¿Por qué la Protección de Datos Personales es una garantía básica de los Derechos fundamentales?", en Revista Electrónica de Derecho Informático N° 38 de septiembre de 2001, cuyo texto se encuentra en http://vlex.com/redi/No._38_-_Septiembre_del_2001/14

26.- JIJENA LEIVA Renato, "Chile, la protección penal de la intimidad y el delito informático", Editorial Jurídica de Chile, Santiago, 1992.

27.- JIJENA LEIVA Renato, "La nueva ley chilena de protección de datos personales, N°19.628 del 28 de agosto de 1999", informe legal, 1999.

28.- JIJENA LEIVA Renato, "Internet, privacidad y derecho, un desafío de cara al siglo XXI en el marco de la globalización", en Revista Electrónica de Derecho Informático N° 36 de julio de 2001, cuyo texto se encuentra en http://vlex.com/redi/No._36_-_Julio_del_2001/3

29.- JIJENA LEIVA Renato, "Responsabilidad de los ISP por la difusión de contenidos on line".

30.- KAISER Pierre, "La protection de la vie privée", Presses Universitaires d'Aix-Marseille, 2e Edition, 1990.

31.- LEMLEY Mark, "Law of the Internet".

32.- LEÓN LEÓN Carlos Alfredo, "Perú: Consideraciones Legales Relativas al Envío de E.mails Comerciales No Solicitados", en Revista Electrónica de Derecho Electrónico N° 36 de julio de 2001, de texto se encuentra publicado en http://vlex.com/redi/No._36_-_Julio_del_2001/13

33.- LLANEZA GONZÁLEZ Paloma, "Internet y Comunicaciones Digitales", Editorial Bosch, Barcelona, España, 2000.

34.- MANTONI Luis María, “El derecho a la intimidad”, Edit Trivium. Madrid, 1983.

35.- Manual Del Usuario de Internet Explorer 6.0.

36.- MARTÍN Lucien, “Le secret de la vie privée, Revue Trimestrelle de Droit Civil”, LVII, T.57, an 1959.

37.- MENDOZA LUNA Amílcar, “Los Cookies ¿Amenaza a la privacidad de información en la internet?”, en Revista Electrónica de Derecho Informático N° 30 de enero de 2001, cuyo texto se encuentra en http://vlex.com/redi/No._30_-_Enero_del_2001/8

38.- MOEYKENS Federico Rafael y SALTOR Carlos Eduardo, “Argentina: La protección de Datos Personales en el Proyecto del Código Civil unificado con el Código de Comercio de la República de Argentina”, en Revista Electrónica de Derecho Informático N° 23 de junio del 2000, cuya texto se encuentra en http://publicaciones.derecho.org/redi/No._23_-_Junio_del_2000/9

39.- NOVOA MONREAL Eduardo, “Derecho a la vida privada y Libertad de Información”, Siglo XXI Editores SA de CV, México D.F., cuarta edición, 1989.

40.- NÚÑEZ PONCE Julio, “La acción constitucional de Habeas Data y la comercialización de información judicial”, en Revista Electrónica de Derecho Informático N° 13, cuyo texto se encuentra enhttp://publicaciones.derecho.org/redi/No._23_-_Junio_del_2000/9

41.- ORTÚZAR VILLAROEL María Carolina, “El nuevo concepto de Derecho a la Intimidad y su protección en la era tecnológica”, Tesis de grado de la Escuela de Derecho de la Universidad Católica de Valparaíso, 1996.

42.- PÉREZ LUÑO Antonio E. (director de la edición), DENNINGER Erhard, “Problemas actuales de la documentación y la informática jurídica”, Editorial Tecnos S.A., Madrid, 1987.

43.- PÉREZ LUÑO Antonio E., “Los derechos humanos en la sociedad tecnológica”, Editorial CEC, Madrid, 1989.

44.- PÉREZ LUÑO Antonio E., LOSANO Mario, GUERRERO María Fernanda, “Libertad informática y leyes de protección de datos personales”, Centro de Estudios Constitucionales. Madrid-España. 1989.

45.- PÉREZ LUÑO Antonio E., “Del “habeas corpus” al “habeas data””, Editorial Aranzadi, Madrid, 1990-1991.

46.- PUCCINELLI Oscar, “El Habeas Data en Indoiberoamérica”, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1999.

47.- RAMOS SUÁREZ Fernando, “¿Es legal el uso de Cookies?”, en Revista Electrónica de Derecho Informático N° 1 de agosto de 1998, cuyo texto se encuentra publicado en http://vlex.com/redi/No._01_-_Agosto_de_1998/ramos

48.- RAMOS SUÁREZ Fernando, “ESPAÑA: Implicaciones jurídicas de la tecnología UMTS”, en Revista Electrónica de Derecho Informático N° 30 de enero de 2001, cuyo texto se encuentra publicado en http://vlex.com/redi/No._30_-_Enero_del_2001/2

49.- ROSENBAUM James M., “Ante todo, privacidad”, en la Columna de Opinión del diario argentino Clarín de fecha 5 de diciembre de 2001.

50.- ROSEMBERG HOLCBLAT Alexander y SÁNCHEZ SANZ Moirah, “El derecho a la privacidad en internet”, en Revista Electrónica de Derecho Informático N°37 de agosto de 2001, cuyo texto se encuentra en http://vlex.com/redi/No._37_-_Agosto_del_2001/5

51.- SÁNCHEZ ALMEIDA Carlos, “España: Intimidad: Un derecho en Crisis. La Erosión de la Privacidad”, en Revista Electrónica de Derecho Informático N° 24 de julio de 2000, cuyo texto se encuentra publicado en http://publicaciones.derecho.org/redi/No._24_-_Julio_del_2000/20

52.- SÁNCHEZ BRAVO Álvaro, “La protección del derecho a la libertad informática en la Unión Europea”, Universidad de Sevilla, Secretariado de publicaciones. Sevilla-España. 1998.

53.- SOBRINO Waldo Augusto Roberto, “Argentina: Las “Cookies” y el “Spam” (y la violación de la “Privacidad” y la “Intimidad”). Un análisis desde la óptica del derecho argentino”, en Revista Electrónica de Derecho Informático N° 35 de junio de 2001, cuyo texto se encuentra en http://vlex.com/redi/No._35_-_Junio_del_2001/3

54.- SUÑE LLINÁS Emilio, “Tratado de Derecho Informático”, Vol. I, Universidad Complutense, Madrid-España. 2000.

55.- URABAYEN Miguel, “Vida privada e información: un conflicto permanente”, Ediciones Universidad de Navarra S.A., Pamplona, 1997.

56.-URIOSTE Mercedes, “Protección de datos personales”, en Revista Electrónica de Derecho Informático N° 23 de junio del 2000, cuyo texto completo se encuentra en http://comunidad.derecho.org/redi/Habeas6.zip

57.- VALLEPUGA GONZÁLEZ Paula, “Responsabilidad de los Prestadores de Servicio en la Sociedad de la Información”, en Revista Electrónica de Derecho Informático N° 41, cuyo texto se encuentra publicado en http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107810

58.- VIAL SOLAR Tomás, “El derecho a la vida privada y a la libertad de expresión en las constituciones de Chile y España: una propuesta de criterios de análisis”, Tesis para optar al grado de Magíster en derecho público de la Facultad de Derecho de la Pontificia Universidad Católica de Chile.

59.- VILLATE Javier, “P3P, un estándar para la privacidad. ¿Es lo que necesitamos?”, en Revista Electrónica de Derecho Informático N° 1 de agosto de 1998, cuyo texto se encuentra publicado en http://vlex.com/redi/No._01_-_Agosto_de_1998/villate

60.- VIVANCO Ángela, “Las libertades de Opinión y de Información”, Editorial Andrés Bello, Santiago de Chile, 1992.

61.- WARREN Samuel y BRANDEIS Louis, “El derecho a la intimidad”, Editorial Civitas, Madrid, 1995.

62.- ZÚNIGA LIRA Paulina, “El Derecho a la Intimidad y la Protección de Datos de Carácter Personal”, Tesis de Grado de la Facultad de Derecho de la Pontificia Universidad Católica de Chile, 1999.

PÁGINAS DE INTERNET VISITADAS:

1.- http://www.cepc.es

2.- www.congreso.cl

3.- http://www.estudionuner.com.ar/legislacion.htm

4.- http://www.ati.es/novatica/glosario/glosario_internet.html

5.- http://www.simil.com/casdeiro/internet/hist.htm

6.- http://www.informaticamilenium.com.mx/Paginas/espanol/sitioweb.htm

7.- http://www.bogote.com/infob/b-net.ht

8.- http://dois.mimas.ac.uk/DoIS/data/Papers/julmjoifp3964.html

9.- http://www.intec.edu.do/redintec/manual_internet/internet.html

10.- http://www.baluma.com/internet1al10/servicios.asp

11.- www.baquia.com

12.- http://zeus.bna.com/e-law/cases/aolcyb2.html

13.- http://v2.vlex.com/es/asp/noticias_detalle.asp?Articulo=118803

14.- http://v2.vlex.com/es/asp/noticias_detalle.asp?Articulo=118372

15.- http://www.libertaddigital.com/suplementos/pdf/anteproyecto_lssice.pdf

16.- http://www.ciberestrella.com/010309/articulos/hotmail.ht5m

17.- http://v2.vlex.com/vlex2/front/asp/noticias_detalle.asp?Articulo=101960

18.- http://www.newsbytes.com

19.- www.elpais.es

20.- http://www.elmundo.es/navegante/2001/12/07/seguridad/1007715325.html

21.- http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=106971

22.- http://www.elmundo.es/navegante/2001/11/26/esociedad/1006801495.html

23.- www.noticias.com

24.- http://www.lun.cl/librerias/prt_em.asp?idnoticia=C37289942337963

25.- www.emol.cl

26.- http://seguridad.internautas.org/criptografia.php

27.- www.kriptopolis.com

28.- http://ulpiano.com/Recursos_Privacy_LatinAmerica.htm

AGRADECIMIENTOS:

-A Miguel Ángel Fernández González, mi profesor guía en ese trabajo, por su buenísima buena voluntad y su paciencia.

-A todos quienes participan en el foro de debate sobre privacidad a través de Internet, cuya dirección es habeasdata@gruposyahoo.com.ar, quienes a través del generoso intercambio de información que en este sitio se realiza, han hecho posible que este trabajo sea un poco más completo.

ÍNDICE

SEGUNDA PARTE:
INTIMIDAD Y TECNOLOGÍA