UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE DERECHO

DIVISION DE ESTUDIOS DE POSGRADO

"REGULACION EN MEXICO DE LA PROTECCION A LA VIDA PRIVADA EN INTERNET"

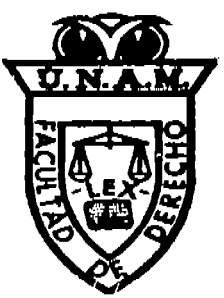
T E S I S

QUE PARA OBTENER EL GRADO DE:

MAESTRO EN DERECHO

P R E S E N T A :

LIC. LUIS JIMENEZ GUZMAN



DIRECTOR DE TESIS: DR. FERNANDO FLORES TREJO

CIUDAD UNIVERSITARIA. 2007

A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO Y A LOS TRIBUNALES AGRARIOS

ÍNDICE

REGULACIÓN EN MÉXICO DE LA PROTECCIÓN A LA VIDA PRIVADA EN INTERNET.

INTRODUCCIÓN

INTRODUCCIÓN

La protección de datos personales y la confidencialidad de la información en Internet, son temas de capital importancia en la sociedad de la información y cada día requieren de mayor atención por parte de la comunidad mundial de Internet; desde los Proveedores de Servicios de Internet (ISPs o *Internet Service Providers*), los responsables o administradores de páginas y sitios *web,* los dueños de empresas con sitios *web,* así como los millones de usuarios alrededor del mundo que deben considerar un código ético en el manejo de la información confidencial a la que tienen acceso y contemplar los ordenamientos jurídicos existentes.

Lo verdaderamente importante es el hecho de que al proteger los datos personales y su confidencialidad, se protege a su titular; de ahí que cuidar la información y hacer un buen uso de ella, es una garantía para proteger a las personas, lo cual se integra dentro de los derechos fundamentales.

En este sentido, el ordenamiento jurídico busca un sistema de protección de datos que sancione la utilización de datos por terceras personas, que sin autorización explícita del titular, puedan ser accesibles a otras personas y/o a una alteración por medio de equipos electrónicos, y provocar daños en lo personal, familiar, social o profesional del individuo al que se le transgredió su intimidad. Los datos personales pueden revelar información sensible de los ciudadanos a saber: nombre, religión, afiliación política, edad, domicilio, finanzas, nacionalidad, educación, historia clínica, estado civil, preferencias sexuales, hábitos de consumo, origen racial, antecedentes penales entre otros, que pueden ser motivo de violación de varios derechos fundamentales como puede ser en el siguiente orden: al conocer nuestras finanzas, somos objeto de secuestros, fraude u ofertas de inversión o crédito no solicitadas, al conocer nuestro origen racial, preferencias sexuales, historia clínica podemos ser objeto de chantaje o discriminación, al conocer nuestro historial crediticio se nos niega el acceso a bienes y servicios y al conocer los hábitos de consumo se nos enviara publicidad no solicitada. Es notoria la importancia que revierte esta información para salvaguardar los derechos inherentes al ciudadano.

La Declaración Universal de los Derechos Humanos, artículo 12, señala que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."; en esta misma declaración, en su artículo 8º se fundamenta que "Toda persona tiene derecho a un recurso efectivo ante los tribunales nacionales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la constitución o por la ley.", esto debe, sin lugar a dudas hacerse extensivo a Internet.

En suma, el objetivo es garantizarle al titular de los datos, que terceras personas, bien se trate del sector público o del sector privado, utilicen la información personal de sus clientes, afiliados, derechohabientes o apoderados

con la confidencialidad que el propietario de la información necesita, de tal manera que el usuario no pierda el control de los mismos, y en todo momento sepa quién tiene sus datos, para qué los utiliza o a quién se los cede o comunica. Es importante señalar que los datos personales a los que se hace referencia aquí, son entre otros, aquellos que se nos solicitan en sitios Web que ofrecen productos y servicios, y en los mensajes electrónicos enviados por correo.

En nuestro país existen algunos casos de importancia en este rubro que han acaparado la atención de los medios por lo que se refiere al respeto a la vida privada. En primer lugar la persecución de las compañías que sin consentimiento de los titulares de los datos, hicieron uso de varias bases de datos como lo es el padrón electoral mexicano, el registro federal de vehículos entre otras bases de datos para venderlos a la compañía norteamericana *Choicepoint* y otras, que son proveedoras del gobierno de los Estados Unidos, especialmente de la agencia gubernamental *Inmigration and Naturalization Service* (Servicio de Inmigración y Naturalización), hechos que están ampliamente documentados por la prensa nacional e internacional. El segundo referente se relaciona a las medidas de control de fronteras de México con Estados Unidos, ya que la lucha contra el terrorismo ha adquirido inusitada importancia, y ha obligado a tomar medidas recientes como la identificación biométrica, así como la crítica el gobierno de los Estados Unidos a la seguridad de los documentos de identificación consular expedidos por el Gobierno mexicano. En este orden de ideas la regulación a la vida privada y en particular a su rastro en Internet esta completamente olvidada en nuestro país, pero los anteriores sucesos ponen el tema en el tintero y nos hacen reflexionar sobre lo que no se ha hecho en nuestro país.

En Iberoamérica sólo existen ocho países con un apartado en su sistema de régimen legal o jurídico de protección de datos personales. Argentina, Colombia, Costa Rica, Chile, España, Perú, Portugal y Uruguay son los estados nacionales que han previsto una discusión sobre su importancia.

Así, en el caso específico de México, se tiene contemplada la Iniciativa de la Ley Federal de Protección de Datos Personales, presentada en febrero de 2001 a la Sesión de la Comisión Permanente de la Cámara de Diputados, si bien no la única, si la más comentada, que señala la necesidad de contener los efectos nocivos de las nuevas tecnologías sobre los tres derechos fundamentales de las personas: la autonomía, la inviolabilidad y la dignidad de la persona. Sobre estos principios, descansa el derecho a la integridad física y moral de la persona, el derecho a que se proteja su intimidad, personal y familiar, y su honor. Esta discusión aun no esta acabada y sobre la misma se tienen que hacer ciertas correcciones y adecuaciones que serían más armónicas con el derecho ya creado en otros países y con la misma legislación interna.

Finalmente es necesario entender el fenómeno en otras latitudes, su evolución y la forma en que ha sido regulado para así poder crear una opinión contundente sobre la materia que venga a aportar soluciones a la discusión aun

vigente. Es por tanto que el desafío por estudiar este fenómeno ha sido el motivo que ha dado pie a las siguientes páginas.

Desde esta perspectiva, en el primer capítulo 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 sus 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 esta 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, en el capítulo segundo, 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 mexicano, que se trata a detalle en el capítulo tercero.

En el cuarto capítulo 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 de la aplicación de este nuevo medio de comunicación.

Explicado esto, en el quinto capítulo, 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 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 en el capítulo sexto, hemos expuesto las principales soluciones que se han puesto sobre la mesa. Para ello, hemos querido que éstas sean conocidas desde dos perspectivas: una tecnológica y otra jurídica.

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. En la novela de Orwell "1984" se habla del "Gran Hermano", una especie de ojo que se encarga de registrar todos los pasos que damos en nuestra vida cotidiana. Aún cuando en la actualidad no hemos llegado a ese extremo de control, no hay duda que sí existen entidades con tendencias *orwellianas,* que amenazan nuestro derecho fundamental a tener una vida privada. No en vano el español Antonio Pérez Luño ha manifestado que se trata de uno de los derechos humanos más vulnerados en la actualidad.

Así las cosas ¿Qué hacer, entonces, para garantizar la adecuada protección de los datos personales, como nos lo exigen los convenios y tratados internacionales, y sobre todo como lo demanda el derecho de los ciudadanos?

Lo ideal sería exigir al legislador que cumpla de forma cabal con su deber; tratándose de derechos fundamentales, no es concebible estar al arbitrio de la potestad de legislar o no; habrá de hacerse, mas al expedir la ya urgente Ley Federal de Protección de Datos Personales para México, acorde con el entorno jurídico internacional, habremos restituido al ciudadano derechos necesarios para un Estado más justo y compatible con un orden social democrático respetuoso de los ciudadanos.

CAPÍTULO PRIMERO

EVOLUCIÓN HISTÓRICA Y CONCEPTUAL DEL DERECHO A LA VIDA PRIVADA

"La historia de la tecnología es también la historia de la invasión de la vida privada"
Mark Lemley

CAPÍTULO PRIMERO. 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 reconocimiento, 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 haya evolucionado de manera radical en relación a sus primeras manifestaciones, tema que será tratado a continuación.

I.- Evolución histórica de la protección de la vida privada

1.- 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 así 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".[1] En la sociedad ateniense, una filosofía parecida cobró y también relevancia en el

[1] MOEYKENS Rafael Federico y SALTOR Carlos Eduardo, en Argentina: ***La protección de Datos Personales en el Proyecto de Códigos Civil unificado de la República Argentina***, Revista Electrónica de Derecho Informático. Número 023, junio de 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=486

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 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."[2]

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.[3] Se refiere al encuentro del hombre y de su relación con el ser supremo. La culminación del pensamiento medieval cristiano está dada 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. 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

[2] Ibídem.
[3] Mateo 20.

pasaje de la confesión pública a la confesión 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.[4]

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 continuo 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".[5] Pocos años más tarde, en 1356, se comenzaría a considerar la buena fama y la posición social, apareciendo las leyes de difamación y libelo.

2.- Del Renacimiento al Siglo de las Luces

Entre el periodo que va desde el Renacimiento hasta el Siglo de las Luces, tomaría forma paralelamente la aparición de la vida pública de la 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, lograron 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[6]. 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. 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

---

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

[5] Ver intimidad, pág. 23, nota 3. de WARREN, Samuel y BRANDEIS, Louis, ***El derecho a la Intimidad***, Editorial Civitas, Madrid, 1995, pág. 13

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

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 "auto dirección 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."[7] Por su parte, Benigno Pendás, refiriendose 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.*"[8]

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 Rebenque, Jeremy Berntham, o al francés Alexis de Tocqueville. Sin embargo, soy partidario 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 respeto 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" [9] 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 vida 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 su pariente quería que se guardaran 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 podría desconocerse sin herir los sentimientos más íntimos y los más respetables de la naturaleza y de la piedad doméstica."[10]

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

---

[7] CASTILLO MARCANO, José Luis, ***El Derecho a la Intimidad y la Protección de Datos Personales en el Derecho Español***, Boletín de la Academia de Ciencia Políticas y Sociales. No. 134. Año LXIV, Caracas, 1997, pág. 8.

[8] WARREN, Samuel y BRANDEIS, Louis, ***El derecho a la Intimidad***, Editorial Civitas, Madrid, 1995, pág. 13, Introducción de PENDÁS, Benigno.

[9] Citado por MANTONI, Luis María, en ***El derecho a la intimidad***, Editorial Trivium. Madrid, 1983, pág. 319. Ver también COLLARD, Royer, ***De la Liberté de Resse, (Discours)***, Paris, 1949, pág. 98.

[10] Citado por URABAYEN, Miguel, ***Vida Privada e Información: un conflicto permanente***, Pamplona, Ediciones Universidad de Navarra, pág. 152.

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.[11]

El 11 de mayo de 1868 se publicaría la Ley de Prensa de la República Francesa, (en francés *Loi relative a 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".[12] 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 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.

3.- De la Era moderna a la postmoderna

Samuel Danls 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".[13] De cual derivan grandes pautas para la posterior evolución de este derecho.

Este texto tiene como antecedente directo la publicación de 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".[14]

Se dice que este derecho deriva del derecho a la propiedad, del cual Warren y Brandeis hacen una distinción entre los derechos a las propiedades materiales e

---

[11] 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. Robert Bandinter, 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 yo no existe (...) hay, sin embargo, un caso en que la vida privada de un individuo debe caer, después de muerto, en le dominio público. es la suerte del hombre protagonista de la Historia "BANINTER, Robert, ***La drout au respect de la vie privée***, Jurisclasseur Périodique, 1968,V.I., No. 2136. Resulta de gran interés considerar que en las iniciativas presentadas tanto a la Cámara de Diputados como a la de Senadores, no se contempla la protección de los datos personales de las personas fallecidas.

[12] La traducción al francés de este artículo es la siguiente: "*Toute pulication dans un écrit périodique relative a la vie privée constitue une contravention punie d´une amende de cinq cents francs. la poursuite ne pourra etre execée que sur la plainte de la pertie interessée* » Rivier, ***Codes Français et Lois Usuelles***, App. Code Penal, page 20.

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

[14] Ibidem, pág. 24

inmateriales, éstos últimos considerados de amplios ámbitos de aplicación, comprendiendo obviamente el derecho a la reserva, o a ser dejado solo.[15] 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, 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".[16] 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 vs. 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 viento 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".[17]

Resulta sumamente interesante la visión futurista de este juez, ya que prevé 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 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

---

[15] Ibídem, pág. 45
[16] Ibídem, pág. 31
[17] Citado por ROSEMERG HOLCBLAT, Alexander y SANCHEZ SANZ, Moirah, ***El derecho a la privacidad en Internet***, Revista Electrónica de Derecho Informático, No. 37, Agosto de 2001, "http://www.alfa-redi.org/rdi-articulo.shtml?x=770" http://www.alfa-redi.org/rdi-articulo.shtml?x=770

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".[18]

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 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 las personas según diversos factores como su origen, sexo, raza, etc.... Entre 1940 a 1943, la GESTAPO descubrió en este sistema un excelente método par 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 aria), 3 (hombre judío), 4 (mujeres 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 estos sistemas 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 es 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.[19] [20]

---

[18] Ibídem, pág. 10

[19] GALLOUEDEC- GENUYS, Francoise & LEMOINE, Philippe, ***La informatización: riesgos culturales***, Barcelona, Mitre, pp. 47-48.

[20] Al leer una nota publicada en El Economista el día primero de agosto de 2006, que señala que en diciembre del año 2006 arranca en Durango el programa piloto de CURP electrónico: "en el que se incluye un chip que contiene la información personal del ciudadano, fotografía, huellas digitales, firma y expediente clínico", me vino a la mente lo sucedido en la Segunda Guerra Mundial, haciendo un poco de historia, en 1939 el escritor británico George Orwell publicó un libro llamado "1984" en el cual muestra un futuro en el año mencionado, en donde solo hay tres continentes en el mundo, el americano, euroasiático y australiano, los cuales siempre están en guerra entre ellos, por motivo de la guerra, la sociedad le ha dado al gobierno todo el poder sobre la gente la cual pertenece al partido totalitario y es controlada por medio del miedo, la propaganda y el castigo despiadado, el gobierno es llamado "El gran hermano" y en las casas de todas las personas eran instaladas en forma común pantallas que servían para ver la televisión así como para ser vigilados por el gobierno. De esta forma el CURP electrónico funcionará con un chip RFID (siglas de *Radio Frequency IDentification*, en español Identificación por radiofrecuencia) que es un método de almacenamiento y recuperación de datos remotos que usa dispositivos denominados etiquetas o *tags* RFID. Una etiqueta RFID es un dispositivo pequeño, como una pequeña estampa, que puede ser adherida o incorporada a un producto, animal o persona. Las etiquetas RFID contienen antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID.
El servicio de acceso al Metrobus utiliza esta tecnología, por ser un medio de acceso rápido, es por lo cual que las tarjetas usadas se leen por el torniquete al contacto, el chip al ser leído en la maquina expendidora es cargado con crédito y descargado en los torniquetes. Enfocándonos un poco en el funcionamiento del Metrobus, cuando se implementó se dijo que gracias al uso del sistema de acceso, se podría saber cual es la frecuencia de viajeros, los

Después de este periodo, 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 Bassin, quien tanto contribuyó en esto, como el conjunto de derechos y facultades sin las cuales el ser humano no puede desarrollar plenamente su personalidad."[21] A la declaración Universal de los Derechos del Hombre le siguieron un sin número 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 este trabajo.[22]

---

tiempos, que estaciones se usan por persona para poder implementar una mejor operación en el transporte, aumentar el número de autobuses según horarios, etc.

Retomando lo dicho en El Economista, el gobierno federal comienza a hacer uso de esta tecnología, ya que lanzará una tarjeta con el CURP en donde vendrán datos personales del ciudadano, fotografía, huellas digitales, firma y expediente clínico.

Hasta aquí todo parece bien, pero desgraciadamente si buscamos un poco de información sobre este sistema, nos encontramos que en Europa donde se le ha dado seguimiento al asunto del RFID, principalmente en España, en donde se ha logrado clonar un chip RFID y así obtener los datos contenidos en el en forma remota. Es decir tendremos una tarjeta con un chip que tendrá todos mis datos y que es vulnerable a clonación y virus, y lo es a distancia. Nos dice la misma nota: "La tarjeta CURP cuenta con un chip con capacidad de 64 kilobytes que incluye la información personal del ciudadano, fotografía y huellas digitales y firma, así como códigos bi y unidimensionales, cinco monederos electrónicos y procesador de señal de radiofrecuencia, además de realizar compras en negocios e identificarse en el banco, los duranguenses podrán, por ejemplo, almacenar en el chip las recetas que les extiendan en el Seguro Popular, con el cual existe un convenio. Además, la tarjeta CURP servirá para almacenar la información de la atención médica que reciban los ciudadanos en el sector salud, como el expediente clínico, tipo de sangre, alergias, tratamientos especiales, entre otras, las escuelas también darán a conocer las calificaciones de los estudiantes a través de esta tarjeta electrónica, la cual podrá ser consultada por los padres de familia en los diversos kioscos de Internet gubernamentales, se incorporó a la tarjeta un procesador que emite señales de radiofrecuencia que permite detectar la ubicación de la persona, con el auxilio de las corporaciones de seguridad pública que son las que reciben esta información".

Todo esto quiere decir que esta tarjeta tendrá mucha información sobre nosotros, y al mismo tiempo se han detectado fallas en la seguridad de este dispositivo en Internet podemos encontrar paginas que incluyen una guía para hacer un lector RFID por 39 dólares nada mas (Ver: http://www.kriptopolis.org/node/802" http://www.kriptopolis.org/node/802) Con ese lector fácilmente se podrá leer esa información y usarla para varios fines como la suplantación de la identidad, acceder a datos personales y privados, y si se obtiene algún lector/escritor del chip, se podrá cambiar desde la fecha de nacimiento, eliminar las alergias del paciente, agregarle nuevas, cambiar dosis de medicamentos, y muchos otros actos criminales.

Dejando a un lado las vulnerabilidades, es aquí en donde entra el Gran Hermano, ya que la tarjeta nos sirve para hacer compras, llamadas telefónicas, es detectable a distancia, el control del gobierno sobre la población aumenta y se incrementa en forma minuciosa, poniendo en peligro una vez mas la privacidad de las personas que tendrán ese documento de por vida. NOTIMEX, ***Arranca tarjeta CURP electrónica***, El Economista, México, 1 de agosto de 2006.

[21] KAISER, Pierre, ***La protection de la vie privée***, Presses Universitaires d' Aix- Marseille, 2e Edition, 1990, pág 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´l´homme dans les nouvelles Deckarations de ces droits. Initalmente concus comme diuts nècessaires a la vie de l´l´homme en societè, ils cont étendus, dans ces nouvelles Déclarations, aux droits nècessaires a son développment, c´est- a – dire, suivant la définition du Président Bassin, qui a beacoup bontribué a cette extensión, a l´ensambla des droits et des facultés sans lequels l´étre humain ne peut Developer pleinemente sa personnalité*"

[22] Ver capítulo segundo 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 han 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 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 auto limitación y la no injerencia de los poderes públicos en la esfera privada. 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".[23] 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 les 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".[24] 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",[25] 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 ente sí por su incidencia universal en la vida de todos y para realizarse exigen esfuerzos y responsabilidades comunes a escala mundial. Esta última clasificación ha tenido gran aceptación por parte de la doctrina internacional. Respecto de estos derechos fundamentales de tercera generación, Vittorio Frosini mencionado por Sánchez Bravo[26] 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 esto derecho de tercera generación con los valores inherentes a la cultura postmaterialista, que ya no responden a

---

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

[24] Ibídem

[25] 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. p.144

[26] SÁNCHEZ BRAVO, Álvaro, ***La protección del derecho a la libertad informática en la Unión Europea***, Universidad de Sevilla, Secretariado de Publicaciones. Sevilla – España. 1998. p.35

la necesidad de seguridad física o económica, como en las dos generaciones anteriores, sin que se relacionen con la autorrealización personal, adoptando un carácter más expresivo que instrumental.[27]

Dentro de la doctrina nacional, no deja de ser interesante la opinión de Aristeo García González, quién señala que "en esta fase (la de los derechos de tercera generación), y dado el desarrollo tecnológico, toma mayor auge el reconocimiento del derecho a la intimidad surgiendo así nuevos perfiles del mismo y que por ende, exige un reconocimiento en sede constitucional"[28], 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" 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 Alemania 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.

En cuanto a la legislación francesa, otro icono 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 se produjo el daño a repararlo".[29] 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". [30]

También en Francia, el 17 de julio de 1970 entraría en vigencia la Ley 70 – 643, cuyo objetivo sería "fortalecer las garantías protectoras de los derechos fundamentales".[31] 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.

---

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

[28] GARCÍA GONZALEZ, ARISTEO, La ***Protección de Datos Personales, Derecho Fundamental del Siglo XXI***. Un Estudio Comparado. Revista de Derecho Informático, No. 100, Noviembre de 2006, http://www.alfa-redi.org/rdi-articulo.shtml?x=7851

[29] Artículo 1382 de Código ***Civil de la República de Francia***. Código traducido en la siguiente página: http://www.legifrance.gouv.fr/html/codes_traduits/somcives.htm

[30] Ver al respecto NOVOA MONREAL, Eduardo, ***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 CEA EGAÑA, José Luis, Vida pública, vida privada y derecho a la información: acerca del secreto de reserva, Revista de Derecho, Facultad de Ciencia Jurídicas y Sociales, Universidad Austral, Vol. III, No 1-2, diciembre de 1992, pág. 14.

[31] KAISER, Pierre, ***La protetion de la vie privée***, Presses Universitares d' Aix- Marseille, 2e Edition, 1990, pág. 79.

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".[32] 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 promulgación 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 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". [33]

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

---

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

[33] Tribunal Constitucional Alemán, sentencia de 15 de diciembre de 1983, publicada en ***BJC Boletín de Jurisprudencia Constitucional***, número 33, Enero 1984, Publicaciones de las Cortes Generales, Madrid. Trad. Manuel Daranas. pp. 126 - 170.

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 llegado a nuestro país.

Según Renato Jimena 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 un perspectiva socializadora y positiva (ya no es el "derecho a ser dejado a solas")"[34]

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 promulgación 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.

II.- Evolución conceptual del Derecho a la vida privada

1.- Conceptos jurídicos tradicionales

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

[34] JIJENA LEIVA, Renato, ***La nueva ley chilena de protección de datos personales***, No.19.628 del 28 de agosto de 1999, informe legal, pág. 5.

vista, y de mayor relevancia dentro de la doctrina latinoamericana que se produjo en el seno de la Comisión de Estudio de la Nueva Constitución de Chile sobre este tema, discusión que en nuestro país no ha sido abordada.

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".[35]
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 conocido 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." [36]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 ellos, utilizando definiciones, tanto de las leyes, como de la doctrina o la jurisprudencia a nivel nacional como internacional.

A) 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 eorm* (confidentes de sus secretos). De ello se desprende que el significado de esta palabra haga alusión a lo íntimo, secreto, recóndito, profundo, propio.

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: *intimita*.
En francés: *intimité*.

---

[35] Citado por EVANS DE LA CUADRA, Enrique en ***Los derechos Constitucionales. Tomo 1***, Editorial Jurídica de Chile Santiago, 1986, pág. 180
[36] Ibidem

En italiano: *intimita*.[37]
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".[38] Sin embargo, 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".[39]

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."[40]

Fried, [41] en un trabajo de 1970 que lleva por título *An anatomy of values* define a la intimidad como "control sobre la información que nos concierne".

Nelson 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".[42]

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 la vida de las personas, soy de la idea de que es más adecuado hablar del "derecho a ser dejado a solas, a ser dejado en paz", en su obra El Derecho

---

[37] Incluso en italiano se utiliza la palabra "riservatezza". Algunos juristas italianos como F. Bricola hablan de "diritto alla reservatezz", haciendo una distinción entre estos dos términos. Ver también DOGLIOTTI, Massimo. ***Il diritto alla riservatezza in Italia e in Francia: orientamenti dottrinali e giurisprudenziali,*** o BESSONE y GIACOBBE (Eds.) ***Il diritto alla riservatezza in Italia ed in Francia.*** Cedam, Padua 1988, p. 86.

[38] ***Diccionario de la Lengua Española***, Real Academia Española, Vigésima Primera Edición, Madrid, 1992, Pág. 835.

[39] DE CUPIS, Adriano, ***Os direitos da personalidade***, Lisboa, 1961, pág. 129.

[40] BAJO FERNANDEZ, Miguel, ***"El secreto profesional en el proyecto de Código Penal,"*** en Anuario de Derecho Penal, Madrid, 1980, pág. 599.

[41] Cambridge, Ma. Harvard University Press, 1970, pág 21.

[42] Citado por NOVOA MONREAL, Eduardo, ***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.

a la Intimidad[43] 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.

Para Georgina Battle Sales,[44] 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".

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".[45]

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 o afligiéndole. Toda persona tiene derecho a exigir que sus asuntos particulares no sean comentados o escudriñados en público, sin su consentimiento".[46] Cabe destacar que en la Enciclopedia Jurídica Mexicana la voz, intimidad, no arroja resultado alguno.

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".[47] 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[48] 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."

Dentro de la doctrina nacional encontramos tres opiniones destacadas de juristas que han tratado de explicar lo que es la intimidad.

El maestro de Derecho a la Información en la Universidad Iberoamericana, Antonio M. Aveleyra considera que la intimidad son aquellas "zonas de reserva

---

[43] WARREN, Samuel y BRANDEIS, Louis, ***El Derecho a la Intimidad***, Editorial Civitas, Madrid, 1995, pág. 21, y 61 y siguientes.
[44] ***Las convenciones ilícitas en los negocios mercantiles***, Revista de Derecho Mercantil, Universidad La Rioja, No. 205, 1992, pág. 449.
[45] NÚÑEZ PONCE, Julio, ***La acción constitucional de Habeas Datas y la comercialización de información judicial***, Revista de Derecho Informático, No. 13, Agosto de 1999,
http://www.alfa-redi.org/rdi-articulo.shtml?x=316
[46] ***Enciclopedia Jurídica Omeba***, Tomo XVI. Editorial Bibliográfica Argentina, S.R. L., Buenos Aires, 1962.
[47] Citado por NOVOA MONREAL, Eduardo, ***Derecho a la vida privada y Libertad de Información***, Siglo XXI Editores SA de CV, México D.F., cuarta edición, 1989, pág. 33
[48] ***Estudios sobre el derecho a la intimidad***, Editorial Tecnos, Madrid, 1992, pág. 88.

de la vida, especialmente la familiar, pero también la vida amistosa y la reserva de la persona a su vida privada vinculada a sus grupos de pertenencia (profesional, político, comunitario, religioso o de cualquier otra asociación o grupo intermedio entre el individuo, el Estado, las entidades supranacionales, o la comunidad universal como totalidad)."[49]

Para el ex-senador y doctrinario en la materia Antonio García Torres, la intimidad: "supone el derecho a la no interferencia de otros en la propia esfera personal y familiar".[50]

El doctor Fernando Flores Trejo, en su obra Bioderecho, primera que aborda tema tan interesante y complejo dentro de la doctrina nacional, al hacer la enunciación de los principios autónomos que comparte tan novísima disciplina, con otras ciencias como la Física o la Química, nos habla del principio de la intimidad individual del cual hemos hecho una interpretación para obtener lo que para el sería el concepto de intimidad: "es la condición personalísima del ámbito interior de cualquier persona" y además este principio ya contiene una medida de protección al señalar que "implica la imposibilidad de intromisión o perturbación de cualquier ente-agente en el fuero interno del ser humano sin que exista autorización expresa de la persona o en su caso una orden judicial."[51]

Por último Ernesto Garzón Valdés, nos dice sobre la intimidad: "es donde el individuo ejerce plenamente su autonomía personal; es el reducto último de la personalidad, es allí donde soy lo que soy."[52]

B) 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 *in 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. El término *privacy*, que en inglés significa "*The right to be let alone; the right of a person to be free from unwarranted publicity.*[53] *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"* [54]También se define la palabra "privado", que en sus diferentes acepciones significa "que se ejecute a vista de

---

[49] AVELEYRA M. Antonio, ***La transición democrática en México, el derecho a la libertad informática, y el derecho a la intimidad***, México, 2002, http://profesor.sis.uia.mx/aveleyra/comunica/privacidad/tdm.htm

[50] ***Exposición de motivos de la Iniciativa que contiene el proyecto de decreto que reforma el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos***, Gaceta Parlamentaria, No. 164, 2006, del Miércoles 5 de abril de 2006.

[51] FLORES TREJO, Fernando, ***Bioderecho***, Editorial Porrúa, México, 2004, pág. 177.

[52] GARZÓN VALDÉS, Ernesto, ***Lo íntimo, lo privado y lo público***, Cuadernos de Transparencia 06, IFAI, México, 2005, pág. 16

[53] Definición obtenida del ***Black´s Law Dictionary***, The Publishers Editorial Staff, St. Paul Minn, West Publishng Co, 1979, pág. 1075

[54] Ibídem.

pocos, familiar o domésticamente, sin formalidad ni ceremonia alguna" particular y personal de cada uno".[55]

La obra de Alan F. Westin 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".[56] En opinión personal, 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:

Soledad.- de orden físico, excluye cualquier contacto material; es el último estado de la *"privacy"*.

"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.

Anonimato.- que implica la falta de identificación, pero que se produce dentro del grupo.

Reserva.- el estado más sutil de la intimidad, que supone la erección de una barrera psicológica frente a intromisiones.

Para Lusky, la privacidad o *privacy* "más que un mero sentido estático de la defensa de la vida privada del conocimiento ajeno, tiene una función dinámica de posibilidad de controlar la circulación de informaciones relevantes para cada sujeto".[57]

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".[58]

Davara Rodríguez define a la privacidad como "término al que podamos 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 tiene mayor trascendencia, pero que al unirlos a otros pueden configurar un perfil determinado sobre una o varias características del individuo que éste tiene

---

[55] ***Diccionario de la Lengua Española***, Real Academia Española, Vigésima Primera Edición, Madrid, 1992, pág.1183.
[56] WESTIN, Alan F. ***Privacy and Freedom***, N.Y. Atheneum, New York, 1967, pág. 215.
[57] LUSKY, Louis, ***Invasion of Privacy: A Clarification of Concepts***, Political Science Quarterly,Vol.87, No.2,, junio de 1972, pág. 192-209.
[58] PARKER, Richard, ***A definition of privacy***, Rutger´s Law Review, No 27, 1974, pág. 276.

derecho a exigir que permanezcan en su esfera interna, en ámbito de privacidad".[59]

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". [60]

En la doctrina nacional existe una confusión en relación a los conceptos de intimidad y privacidad, más no es así en el concepto de vida privada como veremos adelante, en este orden de ideas, el sociólogo Fernando Escalante Gonzalbo, realiza una interesante reflexión en relación a la aclaración de ambos conceptos: "ninguna decisión, ningún espacio es absolutamente privado en el sentido de estar por completo en todo momento, bajo todo punto de vista fuera del alcance de la autoridad pública. Lo que hace la ley es restringir y delimitar las circunstancias en que está justificada la intervención. Lo privado tiene una definición objetiva, que se estipula en la ley, lo íntimo es siempre relativo, se refiere al círculo de personas que de manera natural tiene conocimiento de nuestra vida y nuestras decisiones."[61] Aclara así lo que es privado y lo que es la intimidad.

García Torres, únicamente menciona que la privacidad es "el contenido esencial del derecho a la intimidad",[62] esto tratando de explicar que la protección de datos es un derecho diferente a la protección a la intimidad y la privacidad, sin quedar muy claro si uno contiene al otro o son dos derechos diferentes.

C) Concepto de vida privada

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

En alemán: *privat leben*
En francés: *vie privée.*
En inglés: *private life.*
En español: vida privada.

---

[59] DAVARA RODRIGUEZ, Miguel Ángel, ***La Ley española de protección de datos (LORTAD):¿una limitación al uso de la informática para garantizar la intimidad?***, Actualidad Jurídica No. 12, Elcano, Aranzandi, 1992, pág. 77.

[60] CORRAL TALCIANI Hernán, ***Configuración Jurídica del Derecho a la Privacidad II: concepto y delimitación,*** Revista Chilena de Derecho, Vol. 27 No. 2, Sección Estudios. Pp. 331-355.

[61] ESCALANTE GONZALBO, Fernando, El Derecho a la privacidad, Cuadernos de Transparencia 02, IFAI, México, 2004, pág. 23.

[62] ***Exposición de motivos de la Iniciativa que contiene el proyecto de decreto que reforma el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos***, Gaceta Parlamentaria, No. 164, 2006, del Miércoles 5 de abril de 2006.

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". [63] 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.

Dentro de la doctrina, 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". [64]

Enrique Evans de la Cuadra[65] piensa que "el concepto de "vida privada" está directamente vinculado al de "intimidad", a ese ámbito en que el ser humano y la gente de sus efectos 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 efectos, fomentan sus potencialidades humanas para su progreso integra, todo ello sin la intervención o presencia de terceros".

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 pro terceros sin su consentimiento previo". [66]

El concepto de vida privada también ha sido preocupación de la Suprema Corte de Justicia de la Nación, que en tesis jurisprudencial sostuvo:

> "La Ley no da un concepto de vida privada de una manera explícita, pero si puede decirse que lo contiene implícito, toda vez que en los artículos siguientes se refiere a los ataques a la Nación Mexicana, a las entidades políticas que la forman, a las entidades del país y a la sociedad. Para determinar lo que es la vida privada puede acudirse al método de la exclusión y sostener que la vida privada es aquella que no constituye vida pública. Precisando dicho concepto, puede afirmarse que la vida que observan los funcionarios con este carácter, es decir, en el desempeño de su cargo, y que es lo que interesa a la sociedad, se opone a las actividades del individuo como particular, a sus actividades en el hogar y en la familia; esto en la tónica para considerar cuales fueron los ataques que la Ley de Imprenta quiso reprimir en la fracción I y en la IV del artículo 1°. de la Ley de Imprenta[67]. Allí se contiene

---

[63] ***Diccionario de la Lengua Española***, Real Academia Española, vigésima Primaria Edición, Madrid, 1992, pág. 1183.
[64] NOVOA MOREAL, Eduardo, ***Derecho a la vida privada y Libertad de Información***, Siglo XXI Editores SA de CV, México D. F., cuarta edición, 1989, pág. 49.
[65] EVANS DE LA CUADRA, Enrique, ***Los Derechos Constitucionales, Tomo 1***, Editorial Jurídica de Chile, Santiago, 1986, pág. 172
[66] CEA EGAÑA, José, ***Manual de Derecho Constitucional***, Tomo II, pág. 92
[67] El artículo 1º de la Ley de Imprenta contiene lo que son los ataques a la vida privada:

Artículo 1o.- Constituyen ataques a la vida privada:

I. Toda manifestación o expresión maliciosa hecha verbalmente o por señales en presencia de una o más personas, o por medio de manuscrito, o de la imprenta, del dibujo, litografía, fotografía o de cualquier otra manera que expuesta o circulando en público, o transmitida por correo, telégrafo, teléfono, radiotelegrafía o por mensajes, o de cualquier otro modo, exponga a una persona al odio, desprecio o ridículo, o pueda causarle demérito o en su reputación o en sus intereses;

> una limitación a las garantías de los artículos 6°. y 7° constitucionales, pero se refiere a la vida privada, no a la que observan los funcionarios en el desempeño de su cargo."[68]

El Diccionario Jurídico Mexicano, define a la vida privada como la "esfera personal exclusiva, jurídicamente reconocida y garantizada como derecho a todo ser humano, a fin de permitirle conducir una parte de su propia existencia de manera autónoma, independiente y libre de injerencias externas indebidas, en relación con algunas de sus convicciones, decisiones o actividades íntimas, o con sus relaciones o comunicaciones particulares, atributos personales, vida familiar, reserva domiciliaria, etc."[69]

Para Gómez Robledo y Ornelas Nuñez, el concepto de vida privada, lo entienden "como una idea muy extensa y genérica, que va a cubrir todo aquello que no deseamos llegue a ser parte del conocimiento general de una sociedad en particular."[70]

En lo personal el que redacta este trabajo puede definir 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 alteraciones 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".

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".[71]

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.

II. Toda manifestación o expresión maliciosa hecha en los términos y por cualquiera de los medios indicados en la fracción anterior, contra la memoria de un difunto con el propósito o intención de lastimar el honor o la pública estimación de los herederos o descendientes de aquél, que aún vivieren;

III. Todo informe, reportazgo o relación de las audiencias de los jurados o tribunales, en asuntos civiles o penales, cuando refieran hechos falsos o se alteren los verdaderos con el propósito de causar daño a alguna persona, o se hagan, con el mismo objeto, apreciaciones que no estén ameritadas racionalmente por los hechos, siendo éstos verdaderos;

IV. Cuando con una publicación prohibida expresamente por la Ley, se compromete la dignidad o estimación de una persona, exponiéndola al odio, desprecio o ridículo, o a sufrir daños o en su reputación o en sus intereses, ya sean personales o pecuniarios.

[68] ***Semanario Judicial de la Federación***, Sexta Epoca, Tomo VII, pág, 10.

[69] ***Diccionario Jurídico Mexicano***, T. P-Z, Instituto de Investigaciones Jurídicas UNAM, México, 1996, pág. 3238.

[70] GOMEZ ROBLEDO, Alonso y ORNELAS NUÑEZ, Lina, ***Protección de datos personales en México: el caso del Poder Ejecutivo Federal***, Instituto de Investigaciones Jurídicas, UNAM, México, 2006, pág. 6

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

Revisemos las definiciones que tanto la legislación como la doctrina ha dado al concepto de "derecho a la vida privada".

Las 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 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, 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 de 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".[72]

El connotado maestro en Derecho de la Información, Ernesto Villanueva, define al derecho a la vida privada como "el derecho fundamental de los individuos que consiste en no ser interferidos o molestados, por persona o entidad alguna, en el núcleo esencial de las actividades que legítimamente deciden mantener fuera del conocimiento público."[73]

La *Office of Science and Techonology of the Executive Office of the President*, en una reunión sobre privacidad celebrada en 1967 dirían 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".[74]

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 aceptaciones tienen relación con aquella parte de la vida de las personas considerada como especialmente propia o íntima, las segundas son el emparo 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

---

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

[73] VILLANUEVA, Ernesto, ***Derecho de la Información***, Miguel Ángel Porrua, México, 2006, pág. 301.

[74] Dato obtenido de la página en Internet de ***Office of Science and Technology of The United States of America***: http://www.ostp.gov/

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 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.

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,[75] serían sinónimos, partiendo de la base que de ello no se desprende ningún efecto jurídico.

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 de 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".[76]

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 norteamericano Warren y Brandeis, y en la actualidad, dentro de la doctrina francesa, autores como Pierre Kaiser y Henri Mazeud la utilizan con mucha frecuencia.

Dentro de la doctrina alemana, la cual será analizada con más detalle más adelante, la distinción entre los términos antes aludidos también ha encontrado

---

[75] 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.

[76] GONZALEZ GAITANO, Norberto, ***El deber de respeto a la intimidad: información pública y relación social***, Ediciones Universidad de Navarra, Pamplona, 1990, pág. 76.

cabida, de tal suerte que de ellos se desprenden gradaciones dentro de la vida privada y sus aspectos.[77]

En cuanto a las definiciones propiamente tales de estos tres conceptos, soy de lo 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 Institute,* 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".[78]

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".[79]

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 variante 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 ha modificado el concepto del derecho a la privacidad sí que han modificado las formas en que éste puede ser protegido o puesto en peligro".[80]

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 ésos 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 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

---

[77] Ver a este respecto la obra de NOVOA MONREAL, Eduardo, ***Derecho a la vida privada y Libertad de Información.*** Siglo XXI Editores SA de CV, México D.F., cuarta edición, 1989, pág. 47.
[78] Ibídem, pag.34
[79] VIVANCO, Ángela. ***Las libertades de Opinión y de Información***, Editorial Andrés Bello, Santiago, 1992, pág. 219
[80] CASACUBERTA, David, La ***privacidad en los nuevos medios electrónicos. Aspectos éticos y sociales,*** Revista de Derecho Informático, No. 11, Junio de 1999. http://www.alfa-redi.org/rdi-articulo.shtml?x=276

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 conforman 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 que 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 l a 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.

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 Jinena Leiva, "ello representaría una ventaja, pues permitiría una constante evolución y adaptación del concepto".[81]

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 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

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

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.[82]

2.- Nuevos conceptos jurídicos derivados de este derecho

Al adentrarse una nueva era en la protección del derecho a la vida privada de las personas, muchos "datos"[83] que a lo mejor hace unos años no tenían relevancia, en la actualidad se ha 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 nacio 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".[84] 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

---

[82] La doctrina alemana distingue entra la esfera privada (*privatsphare*), la confidencial (*vertrauensphara*) y la esfera del secreto (*geheimsphare*). Frossini, en Italia, a su turno, distingue cuatro modalidades del aislamiento: la soledad, la intimidad, el anonimato y la reserva. Por último, W. Prosser, en la doctrina norteamericana distingue los siguientes *torts* a la privacidad: intrusión en la vida privada, divulgación de actos privados, divulgación de hechos que originan una falsa imagen pública y apropiación indebida para provecho propio del nombre o imagen ajena. Al respecto ver, NOVOA MONREAL, Eduardo, Op. cit. También PEÑA C, ***Sistema Jurídico y Derechos Humanos***, Cuaderno de Análisis Jurídico, Universidad Diego Portales, 1996.

[83] Debe entenderse como dato al "antecedente necesario para llegar la 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

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

necesariamente con la protección de la intimidad individual."[85] Son partidarios de esta postura Cifuentes y Lucas Murillo.[86]

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 la expresión "protección de datos". Otros autores creen que tal diferenciación es inútil, porque, como lo cita la propia Estadella Yuste, "*data protection is replacing privacy because it indicates a more mundane legal context than human rights*".[87]

En lo personal soy partidario de la postura de Puccinelli, [88] 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". Veamos en todo caso a continuación las distintas definiciones que la doctrina ha dado a esta nueva rama del derecho a la intimidad.

A) 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 tiende, como pareciera seguir 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".[89]

Para el Maestro español Miguel Ángel Dávara Rodríguez, define la expresión protección de datos como: "el amparo debido a los ciudadanos contra la posible

---

[85] ESTADELLA YUSTE, Olga ***"La Protección de la Intimidad frente a la Transmisión Internacional de Datos Personales"*** Centre d'Investigació de la Comunicació, Generalitat de Catalunya. Editorial Tecnos. Madrid, 1995. pág. 81

[86] Ver, CIFUENTES, Eduardo, ***El habeas data en Colombia***, en Derecho a la autodeterminación informativa y acción de Hábeas Data en Iberoamérica, Revista Ius et Praxis, año 3 No 1, universidad de Talca, Chile, 1997, pp. 288-289 y LUCAS MURILLO DE LA CUEVA, Pablo, ***El derecho a la autodeterminación informativa***, Editorial Tecnos, Madrid, 1990, pág. 25

[87] ESTADELLA YUSTE, Olga. Op. cit. pág. 81.

[88] PUCINELLI, Oscar, Op. cit. pág 65.

[89] Ibidem, pág. 65 y 66.

utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad."[90]

Dentro de la doctrina nacional, en la Iniciativa de adición al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, presentada por el en su momento Senador Antonio García Torres el 5 de abril de 2006, propone que se adicionen dos párrafos al artículo 16 de la Constitución:

"Toda persona tiene derecho a la protección de sus datos personales, así como al derecho de acceder a los mismos y, en su caso, obtener su rectificación, cancelación o destrucción en los términos que fijen las leyes.

La ley puede establecer supuestos de excepción a los principios que rigen el tratamiento de datos, por razones de seguridad nacional, de orden público, seguridad, saludo o para proteger los derechos de tercero."[91]

Ahora bien la Ley Federal de Transparencia y Acceso a al Información Pública Gubernamental, en su artículo 3º define lo que es un dato personal:

"Artículo 3.- Para los efectos de esta Ley se entenderá por:
II. Datos personales: La información concerniente a una persona física, identificada o identificable, entre otras, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de saludo físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad."[92]

Es de suma importancia destacar que en nuestro país solo existe una Ley de Protección de Datos Personales que es la del Estado de Colima. Señala Rocío Ovilla Bueno:[93] "entre los motivos que existían en Colima para la creación de esta ley, es que consideraban que en México la protección de los ciudadanos estaba incompleta." Y que razón tiene ya que aun no contamos con una legislación federal en la materia, en su momento hemos de estudiar a detalle esta legislación y las iniciativas que existen en materia de protección de datos en nuestro país, simplemente cabe señalar que esta ley establece la finalidad de proteger y garantizar la protección de los datos de carácter personal como un derecho fundamental.

---

[90] DÁVARA R, Miguel Ángel, ***Manual de derecho informático***, Aranzandi Editores, Madrid, España, 1997, pág. 47

[91] Iniciativa de adición al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, presentada por el Senador Antonio García Torres (PRI), el 5 de abril de 2006, ***Gaceta Parlamentaria***, No. 164, http://www.senado.gob.mx/sen60/sgsp/gaceta/?sesion=2006/04/05/1&documento=9
Cabe señalar que el dictamen de dicha iniciativa, fue aprobado por 77 votos y 5 abstenciones el día 18 de abril de 2006, mismo que fue turnado a la Cámara de Diputados. Está y otras iniciativas en la materia serán estudiadas con más detalle en el capítulo cuarto de esta obra.

[92] ***Transparencia, acceso ala información y datos personales. Marco Normativo***, Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, IFAI, México, 2004, pág. 13

[93] BUENO OVILLA, Rocío, ***La protección de los datos personales en México***, Editorial Porrúa, México, 2005, colección Breviarios Jurídicos No. 28, pág. 42

B) 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 de forma unánime 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 la personas para conocer y acceder a las informaciones que les concierne, 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]

C) 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,

---

[94] PÉREZ LUÑO, Antonio (director de la edición), ***Problemas actuales de la documentación y la informática jurídica***, en capítulo escrito por DENNINGER, Erhard, 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 PÉREZ LUÑO. Antonio, ***Los derechos humanos en la sociedad tecnológica*** en Cuadernos y debates, Editorial Centro de Estudios Constitucionales, Madrid, 1989 pág. 140

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 mismos 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]

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".[98]

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".[99]

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".[100]

Resulta interesante preguntarse si los conceptos recién descritos pueden considerarse como sinónimos o si en realidad comprende 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".[101]

D) 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

---

[97] BROSINI, Victorio, ***Informática y Derecho***, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1988, pág. 69.
[98] PÉREZ LUÑO, Antonio, Op. cit. pág. 138.
[99] Citados por PUCCINELLI, Oscar en ***El habeas Data en Indoiberoamérica***, , Editorial Temis S. A., Santa Fe de Bogotá, Colombia, pág. 68.
[100] Ibidem, pág. 67
[101] Ibidem, pág. 69.

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.[102] 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".[103]

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 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.
>
> La inviolabilidad de los derechos adquirido 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)".[104]

De este artículo se desprenden ya una serie de principios que formarían parte de lo que representan 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 guarda 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.

---

[102] Ver la definición de "dato", en nota 81.
[103] PUCINELLI, Oscar, Op. cit. pág. 209.
[104] Artículo 129 de la Constitución de Weimar de 1919, traducción del Profesor Benito Aláez Corral, disponible *online*: http://hc.rediris.es/05/constituciones/html/ca1919.htm

En cuanto a la naturaleza jurídica del *habeas data*, muchos le ha 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, así 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".[105]

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.

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 computacional mente".[106]

Resulta interesante mencionar la definición que nos da Marie Claude Mayo, quien utiliza como sinónimo 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 le sean exhibidos; el derecho a que sean rectificados y el derecho de 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, bórralos; si sabes para qué los tienes, dímelo y deja que te lo autorice; si esa información es errónea, déjame rectificarla".[107]

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

---

[105] Citado por PUCCINELLI, Oscar, Op. cit. pág 212.
[106] JIJENA LEIVA, Renato, ***La nueva ley chilena de protección de datos personales***, No.19.628 del 28 de agosto de 1999, informe legal, pág. 6.
[107] PUCCINELLI Oscar, Op. cit, pág 351.

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".[108]

En México existen diferentes opiniones de doctrina sobre este nuevo concepto, Marcia Muñoz de Alba Medrano señala que es un "recurso procesal diseñado para controlar la información personal contenida en bancos de datos, cuyo derecho implica la corrección, la cancelación y la posibilidad de restringir y limitar la circulación de los mismos."[109]

Podemos decir que en la doctrina nacional encontramos un debate interesante en determinar si existe o no el *habeas data* reconocido dentro de nuestro ordenamiento jurídico, así en opinión del Ernesto Villanueva, conceptualiza al *habeas data* "que significa conserva guarda (es decir *habeas*, los datos o información y data que corresponden), es una garantía constitucional, derivada funcionalmente del *habeas corpus* del derecho anglosajón, por lo cual todo individuo tiene garantizado el derecho de acceder a la información que le concierne personalmente, a los efectos de que ella lo dispone, no le sea ajena y pueda actuar en consecuencia de ese conocimiento", es importante recalcar que en la nota al pie número diez Villanueva señala "En México no se tiene este derecho como garantía constitucional".[110] Esta opinión abre un debate en relación a que si la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (a partir de este momento LFTAIPG) contiene el recurso de *habeas data*, a pesar de que no existe un reconocimiento constitucional de dicho medio de defensa, ya que la citada ley en su artículo 50 nos dice:

> El recurso también procederá en los mismos términos cuando:
> I...
> II. La dependencia o entidad se niegue a efectuar modificaciones o correcciones a los datos personales;
> III...
> IV...

Y también por su parte el comisionado del Instituto Federal de Acceso a la Información (a partir de ahora IFAI), Horacio Aguilar Álvarez de Alba, en su

---

[108] PÉREZ LUÑO, Antonio, ***Del habeas corpus al habeas data***, Editorial Aranzadi, Madrid, 1991, pág. 174.
[109] MUÑOZ DE ALBA MEDRANO, Marcia, **"Habeas Data"** en CIENFUEGOS SALGADO, David y MACÍAS VAZQUEZ, María Carmen (coord), Estudios en homenaje a Marcia Muñoz de Alba Medrano, Instituto de Investigaciones Jurídicas, UNAM, México, 2006, pág. 2
[110] VILLANUEVA, Ernesto, ***Derecho de acceso a la comunicación pública en Latinoamérica***, Estudio Introductoria y compilación, Instituto de Investigaciones Jurídicas, UNAM, México, 2003, pág. XXV

ponencia intitulada "La protección de datos personales en México"[111] presentada ante la Suprema Corte de Justicia de la Nación, en septiembre de 2006, afirma que la LFTAIPG contiene el *habeas data*, al señalar: "Desde el 2002 la LFTAIPG, contiene disposiciones en materia de tratamiento de datos personales, así como de acceso y corrección de los mismos (*habeas data*)", más adelante señala que dentro de las funciones del IFAI, está la de "garantizar el procedimiento de acceso y corrección de datos personales (*habeas data)* en ficheros públicos".

Al respecto coincido con la opinión vertida por el comisionado Aguilar Álvarez, en el sentido de que es una garantía procesal de reconocimiento de la libertad personal, que si bien no esta consagrada por la ley fundamental no deja de tener un sustento en la legislación federal, ahora bien, no es un *habeas data* en *stricto sensu*, como lo dijera Marcia Muñoz de Alba[112], en su clasificación de *habeas data*, este sería de tipo rectificador o correctivo cuyo objetivo es corregir informaciones falsas, inexactas o imprecisas, nos faltaría la característica de *habeas data* exclutorio o cancelatorio, que elimina información almacenada en algún banco de datos o sistema de información y el *habeas data* aditivo, que actualiza datos o incluye información. Y para reforzar esta postura Muñoz de Alba destaca antes de la promulgación de la LFTAIPG, "no existe en este país una reglamentación expresa sobre el tema. (el *habeas data*) Aunque existen protecciones indirectas sobre la protección a la privacidad a nivel constitucional en el artículo 6º. Considerando la violación a la correspondencia privada."[113] Por último es importante señalar que la Ley de Protección de Datos del Estado de Colima de junio de 2003,[114] en su artículo 7º hace mención expresa al *habeas data* como una forma de protección a los datos personales, a diferencia de la LFTAIPG, en donde solo es un recurso de impugnación y no propiamente el *habeas data.*

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.

Resulta en todo caso de gran interés remitirse a otros ordenamientos jurídicos,[115] 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.

---

[111] ***Seminario Internacional de Acceso a la Información Judicial y Nuevas Tecnologías***, SCJN, México, Septiembre de 2006, http://200.38.86.53/NR/rdonlyres/268296FA-DE64-441C-91E1-888A72C3A035/0/presentaciondedatospersonales26deseptiembrevfppt.pdf

[112] Op. cit. pág. 5

[113] Ibidem.

[114] ***Ley de Protección de Datos Personales del Estado de Colima***
http://www.ucol.mx/radio/textos/sip-4753.pdf

[115] Al respecto recomiendo la obra ya citada, ***Habeas data***, de MUÑOZ MEDRANO DE ALBA, Marcia.

CAPÍTULO SEGUNDO

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

Luke: "What's in there?
Yoda: Only what you take with you"
Star Wars. The Empire Strikes Back

CAPÍTULO SEGUNDO. 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 Derechos 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 mexicano, los Tratados Internacionales tienen rango constitucional[116] , y no obste decir que el derecho a la vida privada se encuentra contenido en instrumentos internacionales que México ha firmado en materia de derechos humanos. En 1981 los principales instrumentos generales de protección a los derechos humanos fueron ratificados por nuestro país, por lo tanto son derecho positivo, el estudio del fundamento constitucional de este derecho a la vida privada es muy extenso y requiere de un especial análisis que más adelante será abordado. Todos los tratados que serán estudiados de acuerdo con el más reciente criterio de la Suprema Corte de Justicia de la Nación,[117] son derecho interno y se encuentran en un plano de

---

[116] El Artículo 133 de la Constitución Política de los Estados Unidos Mexicanos señala que: "Esta Constitución, las leyes del Congreso de la Unión que emanen de ella y todos los Tratados que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República, con aprobación del Senado, serán la Ley Suprema de toda la Unión. Los jueces de cada Estado se arreglarán a dicha Constitución, leyes y tratados, a pesar de las disposiciones en contrario que pueda haber en las Constituciones o leyes de los Estados." ***Constitución Política de los Estados Unidos Mexicanos***, Secretaría de Gobernación, México, 2005, pág. 156

[117] **TRATADOS INTERNACIONALES. SE UBICAN JERÁRQUICAMENTE POR ENCIMA DE LAS LEYES FEDERALES Y EN UN SEGUNDO PLANO RESPECTO DE LA CONSTITUCIÓN FEDERAL**. Persistentemente en la doctrina se ha formulado la interrogante respecto a la jerarquía de normas en nuestro derecho. Existe unanimidad respecto de que la Constitución Federal es la norma fundamental y que aunque en principio la expresión "... serán la Ley Suprema de toda la Unión ..." parece indicar que no sólo la Carta Magna es la suprema, la objeción es superada por el hecho de que las leyes deben emanar de la Constitución y ser aprobadas por un órgano constituido, como lo es el Congreso de la Unión y de que los tratados deben estar de acuerdo con la Ley Fundamental, lo que claramente indica que sólo la Constitución es la Ley Suprema. El problema respecto a la jerarquía de las demás normas del sistema, ha encontrado en la jurisprudencia y en la doctrina distintas soluciones, entre las que destacan: supremacía del derecho federal frente al local y misma jerarquía de los dos, en sus variantes lisa y llana, y con la existencia de "leyes constitucionales", y la de que será ley suprema la que sea calificada de constitucional. No obstante, esta Suprema Corte de Justicia considera que los tratados internacionales se encuentran en un segundo plano inmediatamente debajo de la Ley Fundamental y por encima del derecho federal y el local. Esta interpretación del artículo 133 constitucional, deriva de que estos compromisos internacionales son asumidos por el Estado mexicano en su conjunto y comprometen a todas sus autoridades frente a la comunidad internacional; por ello se explica que el Constituyente haya facultado al presidente de la República a suscribir los tratados internacionales en su calidad de jefe de Estado y, de la misma manera, el Senado interviene como representante de la voluntad de las entidades federativas y, por medio de su ratificación, obliga a sus autoridades. Otro aspecto importante para considerar esta jerarquía de los tratados, es la relativa a que en esta materia no existe limitación competencial entre la Federación y las entidades federativas, esto es, no se toma en cuenta la competencia federal o local del contenido del tratado, sino que por mandato expreso del propio artículo 133 el presidente de la República y el Senado pueden obligar al Estado mexicano en cualquier materia, independientemente de que para otros efectos ésta sea competencia de las entidades

superioridad respecto de las leyes federales y locales y en plano subordinado respecto de nuestra Constitución.

Es importante lo que nos dice Celis Quintal[118] en relación al reconocimiento del derecho a la vida privada en instrumentos internacionales: "Lamentablemente, el escaso conocimiento que se tiene de los tratados internacionales de los que nuestro país, así como la falta de mecanismos institucionales para hacerlos efectivos a través de la aplicación de derecho interno, impiden su aplicación normativa y, podemos decir que, a la fecha, este derecho reconocido internacionalmente por México es solamente una buena intención." Así las cosas a pesar de tener el sustento jurídico, no se ha podido lograr la consolidación a la protección de este derecho.

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, así como también el desarrollo que ha tenido en el derecho extranjero, para que sirva como pauta para futura legislación y marco referencial.

I.- Tratados y Convenios Internacionales

1.- Organización de las Naciones Unidas (ONU)

A) 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

---

federativas. Como consecuencia de lo anterior, la interpretación del artículo 133 lleva a considerar en un tercer lugar al derecho federal y al local en una misma jerarquía en virtud de lo dispuesto en el artículo 124 de la Ley Fundamental, el cual ordena que "Las facultades que no están expresamente concedidas por esta Constitución a los funcionarios federales, se entienden reservadas a los Estados.". No se pierde de vista que en su anterior conformación, este Máximo Tribunal había adoptado una posición diversa en la tesis P. C/92, publicada en la Gaceta del Semanario Judicial de la Federación, Número 60, correspondiente a diciembre de 1992, página 27, de rubro: "LEYES FEDERALES Y TRATADOS INTERNACIONALES. TIENEN LA MISMA JERARQUÍA NORMATIVA."; sin embargo, este Tribunal Pleno considera oportuno abandonar tal criterio y asumir el que considera la jerarquía superior de los tratados incluso frente al derecho federal.
Amparo en revisión 1475/98. Sindicato Nacional de Controladores de Tránsito Aéreo. 11 de mayo de 1999. Unanimidad de diez votos. Ausente: José Vicente Aguinaco Alemán. Ponente: Humberto Román Palacios. Secretario: Antonio Espinoza Rangel.
El Tribunal Pleno, en su sesión privada celebrada el veintiocho de octubre en curso, aprobó, con el número LXXVII/1999, la tesis aislada que antecede; y determinó que la votación es idónea para integrar tesis jurisprudencial. México, Distrito Federal, a veintiocho de octubre de mil novecientos noventa y nueve.
Nota: Esta tesis abandona el criterio sustentado en la tesis P. C/92, publicada en la Gaceta del Semanario Judicial de la Federación Número 60, Octava Época, diciembre de 1992, página 27, de rubro: "LEYES FEDERALES Y TRATADOS INTERNACIONALES. TIENEN LA MISMA JERARQUÍA NORMATIVA.".
Semanario Judicial de la Federación y su Gaceta, T. X. Noviembre de 1999, pág. 46

[118] CELIS QUINTAL, Marcos Alejandro, ***La protección a la intimidad como derecho fundamental de los mexicanos***, en CIENFUEGOS SALGADO, David y MACIAS VÁZQUEZ, María Carmen (coords.), ***Estudios en homenaje a Marcia Muñoz de Alba Medrano. Protección a la persona y derechos fundamentales***, México, UNAM, Instituto de Investigaciones Jurídicas, 2006, pág. 100

> su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."[119]

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 Derechos Humanos, puestos 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. [120]

B) Pacto Internacional de Derechos Civiles y Políticos

En 1996, el derecho a la vida privada fue incluido en el Pacto Internacional sobre Derechos 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".[121]

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[122] en la preservación de la privacidad de los individuos.

C) Convención sobre los Derechos del Niño

Esta Convención, partiendo de la base de los principios de libertad, justicia y de paz proclamada 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".[123]

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

---

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

[120] Ver a este respecto la obra de ROSEMBERG HOLCBLAT Alexander y SÁNCHEZ SANZ Moriah, ***El derecho a la privacidad en Internet***, Revista de Derecho Informático, No.37, Agosto de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=770

[121] Organización de las Naciones Unidas. ***Pacto Internacional sobre Derechos Civiles y Políticos***. 1996.

[122] Para el querido maestro Enrique Sánchez Bringas, el poder político se produce en tres hipótesis: "i) Cuando los órganos del Estado o las autoridades se relacionan entre sí en cumplimiento de sus atribuciones; ii) Aquellos casos en que la interacción social relaciona a gobernantes con gobernados, o sea, cuando establecen contacto, por una parte, el Estado, uno de sus órganos o cualquier autoridad, y por la otra, el gobernado, sea un individuo o un grupo o clase social; iii) Cuando los gobernados -individuos o grupos sociales- interaccionan entre sí en función de un objetivo relacionado con el poder del Estado." SANCHEZ BRINGAS, Enrique, ***Derecho Constitucional***, Editorial Porrúa, México, 2006, pág. 12.

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

injerencias arbitrarias o ilegales. De ello se desprenderán una serie de normas internas para garantizar este derecho en los diferentes países miembros.

D) Directrices para la regulación de ficheros automáticos de datos personales[124]

La Asamblea General de las Naciones Unidas, en su 45º edición ordinaria, CAOC A/RES/45/95, de enero de 1991 adoptó una declaración sobre regulación 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 las personas de que se trate, o prestar asistencia humanitaria.
>
> La legislación nacional debería contener una excepción análoga par 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".[125]

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

---

[124] Para un análisis más particularizado ver el trabajo de. EKMEKDJIAN Miguel A y PIZZOLO, Calogero, ***Hábeas data. El derecho a la intimidad frente a la revolución informática***, Depalma, Buenos Aires, 1996, p. 43

[125] 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.

humanos como el derecho a la protección de la vida privada, y libertades fundamentales como la libertad de la autodeterminación informativa.

También la ONU recomienda la creación de una autoridad de control, que incluya tanto a las personas físicas y morales del sector privado como a las del público, hace mucho énfasis en la importancia de adoptar medidas de seguridad, técnicas y jurídicas, que puedan proteger los datos sensibles, que para Rocío Ovilla Bueno, "son aquellos susceptibles de dar lugar a una discriminación ilícita o arbitraria, y que incluye las informaciones sobre los orígenes raciales o étnicos, el color de la piel, la vida sexual, las opiniones políticas, filosóficas u otras como la pertenencia a un sindicato o asociación."[126]

2.- Organización de Estados Americanos (OEA)

A) Declaración Americana de los Derechos y Deberes del Hombre

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".[127]

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".[128]

B) 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.- PROTECCIÓN DE LA HONRA Y DE LA DIGNIDAD
>
> 1.- Toda persona tiene derecho al respecto de su honra y al reconocimiento de su dignidad.

---

[126] BUENO OVILLA, Rocío, ***La protección de los datos personales en México***, Editorial Porrúa, México, 2005, colección Breviarios Jurídicos No. 28, pág. 5

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

[128] ROSEMBERG HOLCBLAT, Alexander y SÁNCHES SANZ, Moriah, Ob. cit. pág. 20

> 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"[129]

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 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."[130]

3.- Organización para la Cooperación y el Desarrollo Económico (OCDE)[131]

El 11 de abril de 1985, la OCDE adoptó la Declaración sobre flujos de datos transfronterizos, dicha declaración abordaba las cuestiones políticas que surgían del flujo de datos personales más allá de las fronteras nacionales como flujos de datos e información sobre actividades comerciales, flujos intraempresariales, servicios de información informatizada, e intercambios científicos y tecnológicos y posteriormente creó una comisión sobre informatización automatizada y privacidad para estudiar una posible revisión de las Directrices de 23 de septiembre de 1980,[132] mismas que tuvieron el carácter de recomendaciones, aunque esta recomendación no tiene valor obligatorio, exhorta a los Estados a vigilar el equilibrio en esta materia. Al decir de Rocío Ovilla, los Estados tienen dos tipos de obligaciones según estas recomendaciones: "i) la obligación de protección de la vida privada y de las libertades individuales, ii) la obligación de garantizar la libre circulación de datos."[133]

Más recientemente, en la conferencia ministerial de la OCDE "Un mundo sin fronteras: determinación del potencial del comercio electrónico",[134] celebrada en 1998 en Ottawa, los ministros reafirmaron "su compromiso sobre la protección de la privacidad de las redes globales para garantizar el respeto de importantes derechos, generar confianza en las redes globales y evitar restricciones innecesarias en los flujos transfronterizos de datos personales." Declararon concretamente que "trabajarían para vincular los diferentes enfoques adoptados por los países miembros con vistas a asegurar la protección de la privacidad en las redes globales basándose en las directrices de privacidad de la OCDE." Durante dicha conferencia los ministros adoptaron una declaración que reafirmaba su compromiso sobre la protección de la

---

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

[130] 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 1980.

[131] México es miembro de la OCDE desde el 18 de mayo de 1994.

[132] Para más información, remitirse a la obra de URIOSTE, Mercedes, ***Protección de Datos Personales***, Revista de Derecho Informático, No. 023, junio de 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=480

[133] BUENO OVILLA, Rocío, ***La protección de los datos personales en México***, Editorial Porrúa, México, 2005, colección Breviarios Jurídicos No. 28, pág. 4

[134] Organización de la Cooperación y el Desarrollo Económico, ***Un mundo sin fronteras: realizando el potencial del comercio electrónico global***', (Ottawa, Canadá) 7-8 octubre 1998.

privacidad en las redes globales y el inicio de acciones para futuros trabajos en este sentido.

4.- La Unión Europea (UE)

A) 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 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".[135]

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 pasaran 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.

B) Convenio 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 28 de enero de 1981 en Estrasburgo y que se remota 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 adecuadamente el derecho de los individuos al respeto de la vida privada, dado el creciente desarrollo de las tecnologías informáticas.[136]

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 Internacional de expertos encargado 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

---

[135] Consejo de Europa, ***Convención Europea de Derechos Humanos***, 3 de septiembre de 1953.

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

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 autorización de datos de carácter personal.[137] 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.

C) Directiva 95/46 sobre la protección de los individuos en relación al procesamiento de datos personales y sobre libre circulación de esos datos.[138]

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) Establecer 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 moderno 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",[139] lo cual impone un grado de presión internacional para

---

[137] Ver también a este respecto los comentarios sobre este convenio de URIOSTE, Mercedes en ***Protección de Datos Personales***, Op. cit.

[138] Unión Europea, ***Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos***, texto completo en:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML

[139] 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,

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 saludo, 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 tratamiento 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 artículo27. 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 organismos: la Comisión de la Comunidad, un Comité de Representantes de los Estados miembros de la unión (y en algunas circunstancias el principio Consejo de la Comunidad) y un *Working Party*[140] que tiene por objeto la protección de las personas respecto al procesamiento de datos personales.

---

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 derechos, 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 "segura 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]". Al decir de Rocío Ovilla: "El artículo 25 de la directiva conlleva muchos problemas de interpretación y de aplicación". Nos ofrece dos ejemplos el primero respecto a la aplicación hacia un país fuera de la Unión Europea: Estados Unidos y el otro una aplicación hacia el interior: Suecia, en el primer caso hace referencia a los datos que requieren después del 11 de septiembre las compañías aereas y al segundo caso nos trata el caso Lindqvist. Para más al respecto consultar su obra: ***La protección de los datos personales en México***, págs. 9-15.

La directiva 96/9 de la Comunidad Europea no sería sino el perfeccionamiento de la Directiva estudiada 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.

D) Directiva 97/66/CE del Parlamento Europeo y del Consejo sobre procesamiento de datos en el sector de las telecomunicaciones dentro de la Comunidad.[141]

Esta Directiva se celebró con fecha 15 de diciembre de 1997, en la cual temas como la regulación del correo electrónico 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 la telecomunicaciones, así como a la libre circulación de tales datos y de los equipos y servicios de telecomunicaciones en la Comunidad."[142]

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,[143] 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".[144]

---

[140] 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 daros personales dentro de la Comunidad. El *Working Party* tiene que publicar u informe anual sobre el procesamiento de datos personales en Europa y en los terceros países (art.30).

[141] Unión Europea, ***Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones***, texto íntegro en la página de Eur-Lex, el Derecho de la Unión Europea, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:ES:HTML

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

[143] 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 Primaria Edición, Madrid, 1992, pág. 1384.

[144] 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 pueda 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".[145]

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 que han cotizado bien dentro de las empresas a nivel mundial.

Existen también la Directiva 2000/31/CE del Parlamento Europeo y del Consejo del 8 de junio de 2000 relativa a ciertos aspectos jurídicos de la sociedad de la información y sobre todo del comercio electrónico en el mercado común, o la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, que trata una serie de temas, como la conservación de los datos de las conexiones por parte de los Estados miembros con fines de vigilancia policía, el envió de mensajes electrónicos no solicitados o *spam* y el uso de *cookies*, pero para el fin de este trabajo hemos agotado las más relevantes en nuestro tema.

5.- Otros documentos Internacionales

A) 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 objetivos 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

[145] Ibídem, artículo undécimo.

personas. Dicha enumeración ha sido calificada por muchos estudiosos del tema como "exitosa" para la época.[146]

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".[147]

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".[148]

B) Proclamación de Teherán de Derechos Humanos de 1968.[149]

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".[150] Según Puccinelli,

---

[146] Se consideraría en esta Conferencia que "el derecho a la 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 hachos penosos de la vida privada, f) el uso del nombre, intimidad o semejanza; g) ser copiado, atisbado, observado y acosado; h) violaciones a su correspondencia; I) abuso de medios de comunicación, escrito u orales; j) revelación de información dada o recibida en virtud del secreto profesional.

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

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

[149] Organización de las Naciones Unidas, ***Proclamación de Teherán***, Proclamada por la Conferencia Internacional de Derechos Humanos en Teherán el 13 de mayo de 1968.

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

uno de los principales aportes de esta Proclamación es que sería la primera vez que se pretendería proteger los datos personales de las personas.[151]

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.

II.- Derecho comparado[152]

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 leyes 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.

1.- Europa

A) Italia

a) Normas constitucionales

La Constitución de la República italiana[153] fue aprobada por la Asamblea Constituyente el 22 de diciembre de 1947, y entró en vigor el 1 de enero de

---

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

[152] Podemos definir al derecho comparado a "la comparación de los diferentes sistemas legales del mundo. La expresión implica una doble actividad en la que el derecho es el objeto y la comparación el proceso." ZWEIGERT, Konrad y KÖTZ, Hein, ***Introducción al Estudio del Derecho Comparado***, Oxford Univeristy Press, México, 2002, pág. 3.

[153] Para mayor información sobre el proceso histórico y contenido de la Constitución de la República de Italia, ver DE VERGOTTINI, Giussepe, ***Derecho Constitucional Comparado***, UNAM y Segretariato Europeo per le Pubblicazioni Scientifiche, México, 2006, págs. 539 a 554.

1948. En sus artículos 13, 14 y 15 desarrolla lo que es el derecho a la libertad personal y a la intimidad.

> "Artículo 13°. 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 previstas por la ley. Es 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 14°. 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 15°. 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".[154]

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 proteger el derecho a la libertad personal, a la inviolabilidad del hogar y a la inviolabilidad de correspondencia, puede deducirse que, por analogía se protege constitucionalmente la intimidad de las personas. Este aparente vacío se verá llenado con las distintas leyes internas, en especial las normas sobre protección de datos recientemente creadas. Este caso es muy parecido al de nuestro país que en su momento será estudiado.

b) Normas Internas

La ley más importante es la N°. 675 del 31 de diciembre de 1996 en Italiano *Tutela delle persone e di altri soggotti rispetto al trattmento dei dati personali*, la cual tiene por objeto adecuar la legislación italiana a la Directiva 95/46/CE. 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 al mencionada ley 675.

---

[154] Artículos 13, 14 y 15 de la ***Constitución de la República Italiana***, de la página web de la Corte constituzionale della Repubblica italiana, http://www.cortecostituzionale.it/esl/testinormativi/costituzionedellarepubblica/costituzione_parte_i.asp

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 o jurídica, autoridad. Organismo o ente público, asociación y organización, que procesa los datos personales en nombre del Controlador (art.1.2.e)."[155]

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, 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 hayan 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 Procesamientos Penal.
>
> 3) Está prohibida la transmisión cuando las leyes y regulaciones del país de destino no garantizan los interesados un adecuado nivel de 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 Procedimiento penal."[156]

---

[155] 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.***

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

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 expuesto de reconocida trayectoria en las disciplinas del derecho o tecnología informática. Duran 4 años en sus funciones, y son reelegibles sólo una vez. Además, su dedicación es exclusiva.[157] Al decir de Celis Quintal, "el derecho a la intimidad en Italia ha llegado tarde. La Ley 675, que tutela la privacidad, es fruto de la presión social y de las obligaciones impuestas por las directivas comunitarias. Sin embargo, el retardo ha traído una pequeña gran ventaja: la ley pudo nacer siguiendo la directiva 95/46/CE, por lo que representa una normativa que lejos de improvisarse, es moderna y fue bien estudiada."[158]

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 Comunicación*, 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 N° 318 o decreto 318/99. Dicho Decreto fue dictado en cumplimiento del mandato de la sección 15, parágrafo segundo, 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/CE), 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

---

[157] 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.***

[158] CELIS QUINTAL, Marcos Alejandro, ***La protección de la intimidad como derecho fundamental de los mexicanos***, en CIENFUEGOS SALGADO, David y MACIAS VAZQUEZ, María Carmen (coord.) ***Estudios en homenaje a Marcia Muñoz de Alba Medrano***, México, Instituto de Investigaciones Jurídicas, UNAM, 2006. pág. 87.

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 (artículos 614 a 623) y de Procedimientos Penales (artículos 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.[159]

Existen también leyes sectoriales relativas a supervisión en los lugares de trabajo (Ley N° 93, del 29 de marzo de 1983, *Legge quadro dul 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.

B) Alemania

a) Normas constitucionales

La Carta Magna germana[160] en su artículo décimo consagra el derecho al secreto de las comunicaciones. No es precisamente un reconocimiento al derecho a la intimidad, sino 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.

---

[159] Información obtenida en el artículo "***Privacy Laws & Business International Data Protección Roundup***", Revista Privacy Laws&Bussines, International Newsletter, N°60, enero de 2002, pág.17

[160] Para mayor información sobre el proceso histórico y contenido de la Constitución de Alemania, ver DE VERGOTTINI, Giussepe, ***Derecho Constitucional Comparado***, UNAM y Segretariato Europeo per le Pubblicazioni Scientifiche, México, 2006, págs. 527 a 539

> "Artículo 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. Sin 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 o 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." [161]

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".

b) 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,[162] cabe señalar que estas fueron las primeras legislaciones en materia de protección de datos en existir. 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

---

[161] La traducción de este artículo en alemán es *"Artikel 10 [Brief-, 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 die dem Betroffenen nicho mitgeteilt wird und daßan die Stelle des Reschtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt"*, ***Grundgesetz für die Bundesrepublik Deutschland***, Deustcher Bundestag (Congreso de la República de Alemania), http://www.bundestag.de/parlament/funktion/gesetze/grundgesetz/

[162] El texto de esta norma puede ser consultado en inglés en la siguiente página de Internet: http://www.luscomp.org/gla/statutes/BDSG.htm ***Federal Data Protection Act*** o en alemán ***Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung***, del 20 de diciembre de 1990 y su reforma el 14 de septiembre de 1994.

> especiales sea mejor prestarlo de otro modo- y estar claramente diferenciado cuando forme parte de otras declaraciones escritas".[163]

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.

> "Sección 18.- Las Supremas Autoridades Federales, el Presidente del 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 trasmiten y sus receptores; periodos estándares para la supresión de datos; grupos de personas que tienen derecho de acceso o las personas que tiene este derecho en forma exclusiva".[164]

Esta norma se vuelve interesante en cuanto a las obligaciones que podrían recaer en los Proveedores de Servicios de Internet, más conocidos como ISP (cuya siglas en Inglés son *Internet Service Porvider*)[165] Así mismo, si acaso los sistemas de procesamiento utilizados tienen relación con Internet, es más fácil controlar el uso que se le está dando a esta poderosa herramienta de almacenamiento y comunicación de información.

---

[163] Sección 4 de la ***Federal Data Protection Act*** de la República de Alemania.
[164] Sección 18 de la ***Federal Data Protection Act*** de la República de Alemania.
[165] Mi definición sobre *Internet Service Providers* es la siguiente: "empresa que comercializa accesos a Internet. Facilitan a los usuarios los códigos que permiten el acceso a la red" JIMENEZ GUZMÁN, Luis, ***Hacia una regulación del Comercio electrónico en México***, Tesis Profesional, México, 2000, pág. 12.

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 de las otras relativas a la protección de datos, cuando tiene suficientes indicaciones de que han sido violadas y, particularmente, cuando el interesado presenta pruebas 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 adaptación 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 esta área.

Recientemente se han aprobado varias normas relativas a la privacidad de las comunicaciones, como la *Telecommunications Carriers Data Protection Ordinance* (TDSV),[166] 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*[167] de primero de agosto 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 telecommunications ordinance (Telelkommunikations- Uberwachungsverordung-TKÜV)*[168], 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.[169]

---

[166] El texto completo de esta ley lo podemos encontrar en la página de IUSCOMP, ***The Comparative Law Society***, http://www.iuscomp.org/gla/statutes/TDSV.htm

[167] Podemos encontrar el texto completo de la presente ley en la página dedicada a legislación alemana denominada, ***Media & Law***, http://www.medialaw.ru/laws/russian_laws/telecom/npa/6etr/germ.htm

[168] El texto completo de esta ley lo podemos encontrar en la página de IUSCOMP, ***The Comparative Law Society***, http://www.iuscomp.org/gla/statutes/TKG.htm

[169] Información obtenida en el artículo ***"Privacy laws & Business International Data Protection Roundup"***, Revista Privacy Laws&Bussines, International Newsletter, N° 60, enero del 2002, pág. 15.

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.[170]

C) Francia

a) Normas constitucionales

La Declaración de los Derechos del Hombre y del Ciudadano de 1789[171], 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".[172]

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.

La Constitución Gala,[173] vigente desde el 4 de octubre de 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.

b) 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 de 17 de julio de 1970 que creó el actual artículo 9 del Código Civil.[174]

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

---

[170] En virtud de lo resuelto por el Tribunal de Justicia de las Comunidades Europeas en el caso Marleasing (del 13-11-90, C-6/90 y C-9/90).

[171] A nivel nacional, la Declaración de Derechos del Hombre y del Ciudadano forma parte, al igual que el Preámbulo de la Constitución de 1946 que la completa, de los textos constitucionales actualmente vigentes bajo el imperio de la Constitución del 4 de octubre de 1958. Los acuerdos internacionales para promover los derechos humanos tienen por lo demás un valor superior al de las leyes y son, muchos de ellos, directamente invocados por particulares frente a las jurisdicciones. La amplitud de la legislación nacional consagrada a los Derechos del Hombre verifica también la importancia fundamental que les atribuye Francia.

[172] Artículo 11 de la ***Declaración de los Derechos del Hombre y del Ciudadano*** de 1789.

[173] Para mayor información sobre el proceso histórico y contenido de la Constitución de Francia, ver DE VERGOTTINI, Giussepe, ***Derecho Constitucional Comparado***, UNAM y Segretariato Europeo per le Pubblicazioni Scientifiche, México, 2006, págs. 514 a 527

[174] El artículo 9 del Código Civil a la letra dice: "Cada uno tiene derecho a que se respete su vida privada.

Sin perjuicio de la reparación del daño sufrido, los jueces podrán prescribir toda clase de medidas tales como secuestro, embargo y demás, propias para impedir o cesar un ataque a la intimidad de la vida privada; en caso de necesidad estas medidas podrán ordenarse por procedimiento de urgencia." ***Legifrance, Le Service Public de l'acces au droit***, http://www.legifrance.gouv.fr/html/codes_traduits/civestxt.htm

1978. Uno de los grandes alcances 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."[175]

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 la 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, los destinatarios de sus datos y la existencia de un derecho de acceso y de rectificación (ésta liberada del cumplimiento de esta exigencia la recolección de la información necesaria para la constatación de infracciones), como lo consagra el artículo 27.

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."[176]

El ente encargado de velar por el adecuado cumplimiento de estas normas es la Autoridad de Control. Ella se conforma por la Comisión Nacional de Informática y de las Libertades[177] (CNIL), autoridad administrativa independiente,

---

[175] Artículo 1 de la ***Ley de Informática, Ficheros y Libertades, o Ley 78-17***, aprobada el 6 de enero de 1978. http://www.legifrance.gouv.fr/WAspad/AJour?nor=&num=78-17&ind=1&laPage=1&demande=ajour

[176] Artículo 24 de la ***Ley de Informática, Ficheros y Libertades, o Ley 78-17***, aprobada el 6 de enero de 1978. http://www.legifrance.gouv.fr/WAspad/AJour?nor=&num=78-17&ind=1&laPage=1&demande=ajour

[177] Al decir de OVILLA BUENO, Rocío, la CNIL, "hoy en día tiene un papel de garante del respeto de los derechos fundamentales", esto es interesante ya que son varias las voces que se pronuncian sobre este derecho como un derecho fundamental y no simplemente un derecho secundario. Op. cit. pág. 19.

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 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.

Cabe mencionar que la ley antes descrita es parcialmente modificada por la ley No 2004-182 del 6 de agosto de 2004 relativa a la protección de las personas físicas con respecto al tratamiento de datos personales, buscando así la armonización que plasma su deseo en la directiva europea 95/46/CE[178] de octubre de 1995. El principal objeto de esta reforma es adaptar la protección brindada por Francia a la evolución de la tecnología y darle más fuerza a la protección de datos obtenidos por sistemas automáticos de recolección de datos, así podemos destacar que esta reforma incorpora la identificación por parte de empleadores mediante la utilización de técnicas biométricas de identificación de los trabajadores y limita el almacenamiento de estos datos sin justificación.

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.[179] .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. 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*.[180] de los ministerios. Este modelo, según la explicación de Mercedes Urioste, junto con la guía distribuida a los responsables

---

[178] 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 Marleasig (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, de acuerdo a lo que el mismo Tribunal resolvió en el caso Francovich (sentencia del 19-11-91, C-6/91, C-6/90), por lo tanto era ya imperativo la implementación de la Directiva en la legislación francesa.

[179] 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 vs. Fmace (caso176-A, Serie A), dio lugar a la aprobación de la ley de 1991. citado por URIOSTE, Mercedes, ***Protección de Datos Personales***, Revista de Derecho Informático, No. 023, junio de 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=480

[180] Se entiende por *site* (sitio) "punto de la red con dirección única y al que pueden acceder los usuarios para obtener información", FERNANDEZ CALVO, Rafael, ***Glosario básico inglés – español para usuarios de Internet***, http://www.ati.es/novatica/glosario/glosario_internet.html#S

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 l 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 posterior mente 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 objetivo, 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 directorio 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 18-597); 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 d 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), archivo (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.

D) Reino Unido

a) Normas constitucionales

Dentro de la Constitución inglesa[181] 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.

b) Normas internas

[181] Para mayor información sobre el proceso histórico y contenido de la Constitución inglesa, ver DE VERGOTTINI, Giussepe, ***Derecho Constitucional Comparado***, UNAM y Segretariato Europeo per le Pubblicazioni Scientifiche, México, 2006, págs. 495 a 506.

La Ley de Protección de Datos o *Data Protection Act*[182] de 1998, aprobada para adecuar la legislación británica a la Directiva 95/46/CE 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 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, deberá 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 corresponde a:

> Primer Principio: los datos personales deben ser procesado 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)[183]
>
> Segundo Principio: los datos personales sólo deben ser procesados para uno o más objetivos específicos y lícitos, y no deben ser procesados para uno o más objetivos específicos y lícitos, y no deben ser ulteriormente procesados en forma incomparable 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).

---

[182] Texto de la ***Data Protection Act***, Public Sector Information UK, http://www.opsi.gov.uk/acts/acts1998/19980029.htm

[183] 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 interesados; b") para la administración de justicia, o para que una persona, la Corona, un Ministro de la Corona o un departamento cumplan una obligación jurídica; b"") proteger los intereses legítimos del Controlador o del tercero a quien los datos se transmiten, excepto 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).

> Cuarto Principio: lo datos personales deben ser exactos y, cuando sea necesario, actualizados (&4 de la Parte I del Primer Anexo).[184]
>
> 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 deben procesarse respetando los derechos que esta ley acuerda a los interesados (&6 de la Parte I del Primer Anexo).[185]

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 cuanta 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".[186]

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

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 sus designaciones 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).

---

[184] 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).

[185] La Parte II de este mismo Anexo dispone que se considere a 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 de 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 de) no accede a una solicitud de que se asegure de que ose están adoptando decisiones automatizadas relativas a su persona (& 8).

[186] Ley de Protección de Datos del Reino Unido, &13 de la Parte II del Primer Anexo.

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[187]. La Ley de Poderes Investigativos (*Regulation of Investigatory Powers Act*),[188] 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 pedofilos 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.[189]

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 pleno 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 las justicia, para preservar y proteger los mismos como evidencias para establecer pruebas en la inocencia o culpabilidad".[190]

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. La ley también ha sido criticada por los PSI británicos por las empresas del campo de la tecnología de la información, puesto que consideran que la Ley, irónicamente llamada RIP por los ingleses[191], facilita demasiado las posibilidades de obtención de la orden judicial necesaria para intervenir cualquier correo electrónico o historial de navegación. Finalmente, cabe destacar que la Ley de Poderes Investigativos establece también en su Sección 4, que cualquier intercepción de una comunicación durante su periodo 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 encuentra 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.

---

[187] Sin mencionar el *"Aviation and transportation security Act"* de los Estados Unidos que será estudiada más adelante.

[188] Texto de la ***Regulation of Investigatory Powers Act***, Public Sector Information UK, http://www.opsi.gov.uk/acts/acts2000/20000023.htm

[189] Ver nota 48 con la definición de ISP.

[190] Citado por ROSEMERG HOLCBLAT, Alexander y SANCHEZ SANZ, Moirah, ***El derecho a la privacidad en Internet***, Revista Electrónica de Derecho Informático, No. 37, Agosto de 2001, "http://www.alfa-redi.org/rdi-articulo.shtml?x=770" http://www.alfa-redi.org/rdi-articulo.shtml?x=770

[191] **RIP** e inglés es el acrónimo de ***Rest In Peace***, que significa "descanse en paz", haciendo alusión a las siglas de la ley: ***Regulation of Investigatory Powers***.

E) España

a) Normas constitucionales

La Constitución española[192] 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."[193]

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 privada de las personas frente a las amenazas que provoca Internet tiene expresamente un resguardo constitucional.

b) 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[194], reemplazó a la antigua LORTAD (Ley Orgánica de Resolución de Tratamiento Automatizado de Datos) de 1992.

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 liberaciones

---

[192] Para mayor información sobre el proceso histórico y contenido de la Constitución de España, ver DE VERGOTTINI, Giussepe, ***Derecho Constitucional Comparado***, UNAM y Segretariato Europeo per le Pubblicazioni Scientifiche, México, 2006, págs. 554 a 566.

[193] Constitución Española aprobada por las Cortes en Sesiones Plenarias del Congreso de los Diputados y del Senado. 31 de Octubre de 1978. Raficada 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

[194] La disposición derogatoria única de la ley 15/99 establece que: "Queda deroga da la Ley Orgánica 5/1992, de Sancionada por S.M. el Rey ante las Corte el 27 de Diciembre de 1978. reformada el 27 de Agosto de 1992.

> públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".[195]

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 honestos 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 la 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.
>
> 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

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

> 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 supuesto de que le afectado esté física o jurídicamente incapacitado para dar su consentimiento."[196]

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 deontológico o de buenas prácticas profesionales, 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).[197]

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. 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".[198]

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 1333/94 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

---

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

[197] 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 transferencias de daros. 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".

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

las Medidas de Seguridad de los Ficheros Automatizados previstas por el Reglamento aprobado por el Real Decreto 994/1999 antes mencionado.

Existe también la Ley de Servicios de la Sociedad de la información y de comercio electrónico del 11 de julio de 2002, que regula las actividades económicas en Internet. Así, establece, según las pautas dictadas por la Unión Europea, una serie de normas para las *webs*[199] de comercio electrónico e incluye una regulación acerca del "*spam*"[200] (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 del Internet, este ordenamiento es un avance notable en esta lucha, así su numeral 21 nos da la siguiente protección:

> Artículo 21. *Prohibición de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes*
>
> 1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.
>
> 2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.
>
> En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

---

[199] 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 es ese caso debería decirse páginas *web* o sitio *web*." FERNANDEZ CALVO, Rafael, ***Glosario básico inglés – español para usuarios de Internet***, http://www.atl.es/novatica/glosario/glosario_internet.html#S

[200] El *spam*, puede ser definido según la propuesta que hace el Decreto S 1618 ES del Senado de los Estados Unidos de Norteamérica, que cabe señalar que nunca se constituyo como una Ley, ya que el mismo fue frenado en la Cámara baja de la Unión Americana y que ha sido utilizado de forma reiterada por distribuidores de *spam* como pretexto de cumplimiento de alguna "normativa" que es al caso inexistente.(ver al respecto el sitio: http://www.cubiro.com/articulos/el_decreto.htm#) En su sección 306 señala: "Correo electrónico comercial.- El término correo electrónico comercial significa cualquier correo electrónico que:

A) Contenga un anuncio comercial que promueva la venta de un producto o servicio
B) Contenga una solicitud del uso de un número telefónico, para anuncia a una persona o corporación la venta de un producto o servicio
C) Promueva el uso o contenido de listas de uno o más sitios de Internet que contengan un anuncio comercial como el señalado en el subpárrafo A) o una solicitud como la señalada en el subpárrafo B)"

Ahora bien en un personal punto de vista y adhiriéndome a al opinión de Jesús Cea Avión, el *spam* no es únicamente un fenómeno comercial con *animus* de lucro, puede ser cualquier otro correo que contenga contenidos de cualquier índole pero sea molesto o invada nuestra esfera de privacidad. JIMÉNEZ GUZMÁN, Luis, ***Hacia una regulación del comercio electrónico en México***, Tesis de Licenciatura, México, 2000, pág 162-163.

Sin embargo, el artículo primero de dicha norma claramente señala que no regulará la protección de datos personales.[201]

2.- América del Norte

A) Estados Unidos de América

a) 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 podrá ser emitida si 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"[202]

Como lo señala Rosemberg y Sánchez Sánz, "el legislador estadounidense separó la 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 a la protección del derecho a la privacidad contra las injerencias del gobierno, y no es extensible al ámbito privado". [203]

La primer sentencia que reconoce el derecho a la intimidad como derecho constitucional, se dio en el caso *Griswold vs. Connecticut* (381 US 479, 1965); en dicha sentencia se declaro inconstitucional la ley del estado de Connecticut que prohibía el uso de anticonceptivos a las personas casadas, considerando tal uso como delictivo, el fallo determino que dicha ley violaba el derecho a la vida

---

[201] La Ley de servicios de la sociedad de la información y de comercio electrónico, en el Título 1 sobre Disposiciones Generales, el Capítulo 1 se refiere a la finalidad y conceptos básicos señalando que: "Artículo 1. *Objeto* 1. Es objeto de la presente Ley la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, 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 se entenderán sin perjuicio de lo dispuesto en otras normas estatales o autonómicas ajenas al ámbito normativo coordinado, o que tengan como finalidad la protección de la salud y seguridad pública, incluida la salvaguarda de la defensa nacional los intereses del consumidor, el régimen tributario aplicable a los servicios de la sociedad de la información, la protección de datos personales y la normativa reguladora de defensa de la competencia." Departamento de Justicia de la Generalitat de Catalunya, ***Ley de servicios de la información y de comercio electrónico***, http://civil.udg.edu/normacivil/estatal/contract/LSSI.htm

[202] Enmiendas IV y V. ***The Constitution of The United States of America***, Applewood Books, Bedford, Massachussets,United States, 2002, pág. 19.

[203] ROSEMBERG HOLCBLAT, Alexander y SÁNCHEZ SANZ, Moirah, ***El derecho a la privacidad en Internet***, Revista de Derecho Informático, No.37, Agosto de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=770

privada de las personas casadas, dicha resolución trajo como consecuencia que las Constituciones de distintos estados establecieran principios relativos a la protección de la privacidad, como lo es la Constitución de California.[204]

b) Normas internas

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 tienen el derecho de acceder a la información personal que de ellos mantenga el gobierno, y de solicitar que cualquier información inexacta sea corregida.

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".[205]

Es preciso recalar 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.[206]

Una de las normas más importante en cuanto a la protección del derecho a la vida privada en Internet es la Ley de Privacidad de las Comunicaciones Electrónicas, o *Electronic Communications Privacy Act*, ECPA[207] 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

---

[204] A este respecto ver CELIS QUINTAL, Marcos Alejandro, ***La protección de la intimidad como derecho fundamental de los mexicanos***, en CIENFUEGOS SALGADO, David y MACIAS VAZQUEZ, María Carmen (coord.) ***Estudios en homenaje a Marcia Muñoz de Alba Medrano***, México, Instituto de Investigaciones Jurídicas, UNAM, 2006.

[205] ROSEMBERG HOLCBLAT, Alexander y SÁNCHEZ SANZ, Moirah, Ibídem, pág. 40.

[206] 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". Op. Cit. pág. 39.

[207] Texto completo disponible en la página de ***U.S. Internet Industry Association***, http://www.usiia.org/legis/ecpa.html

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".[208]

Unos 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.

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*[209]. 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 líneas, y otros. Sin embargo, dicha restricción no prohíbe a los empleados o agentes de servicios de comunicaciones, siempre que estén dentro del curso normal de las actividades inherentes a la prestación del servicio, o la interpretación, uso o revelación obedezcan a la protección de los intereses del proveedor del servicio. Aunque pareciera bastante simple, 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

---

[208] SMEDINGHOFF, Thomas J. ***On-line Law.*** Addison-Wesley Developers Press, United States of America, 2000, pág. 77.

[209] 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". FERNANDEZ CALVO, Rafael, ***Glosario básico inglés – español para usuarios de Internet***, http://www.ati.es/novatica/glosario/glosario_internet.html#S, A este respecto es interesante saber como existe toda una subcultura alrededor de esta actividad, así en 1984 del trabajo de Steven Levy, ***"Hackers: heroes of the Computer Revolution"***, se examina la evolución de la ética hacker, en un sextoto de credos que surgieron de las actividades de los *hackers* "pioneros" a fines de los cincuentas: "1.- Entrégate siempre al imperativo de Transmitir! El acceso a ordenadores y cualquier otra cosa que pueda enseñarte sobre como funciona el mundo debe ser ilimitado y total. 2.- Toda la información debe ser libre. 3.- Desconfía de la autoridad- Promueve la descentralización. 4.- Los *hackers* deben ser juzgado por su *hacking*, no por criterios falsos como títulos, edad, raza o posición. 5.- Puedes crear arte y belleza en un ordenador. 6.- Los ordenadores pueden cambiar tu vida a mejor" Este código ético forma la base política de las actividades de los *hackers* modernos. Dell Books, New York, 1984, pág 26. También en relación a la definición de *hacker* podemos decir que las mismas varían de acuerdo con la posición socio-política del grupo o individuo que lo defina. Así podemos decir que dentro de la subcultura *hacker* se entiende al mismo como: "entusiastas de la informática que tienen un interés ardiente en aprender acerca de los sistemas informáticos y como usarlos de formas innovadoras" según Dorothy Denning, ***Concerning Hackers Who Break Into Computer Systems.*** en *Proceedings of the 13th National Computer Security Conference*, Octubre 1990. Esta definición, por tanto, no incluye a los *hackers* malignos que deliberadamente rompen sistemas y borran ficheros, sino a esos *hackers* que exploran sistemas simplemente por el reto intelectual y que no dejan indicios de sus actos. JIMENEZ GUZMÁN, Luis, ***Hacia una regulación del Comercio electrónico en México***, Tesis Profesional, México, 2000, pág. 132, notas 117, 118 y 119.

electrónica, lo cual también es significativo a la luz del problema del monitoreo de *emails* 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 *Children´s Online Privacy Protection Act* (COPPA),[210] 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*[211], 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 páginas con respecto a la revelación de tal información.

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 par 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 líneas 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.

Es preciso destacar que la creación de leyes de lucha contra el terrorismo, después de los atentados del 11 de septiembre de 2001, ha arrojado ordenamientos fundamentales que violan en algunos sentidos la protección a la vida privada. En primer lugar tenemos la *Aviation and Transportation Security Act*[212] del 19 de noviembre de 2001 que obliga a las aerolíneas a pedir la lista de los pasajeros y la tripulación, donde se cuentan con muchos datos sensibles

---

[210] Texto completo de esta legislación en la página de ***Center for Democracy and Technology***, http://www.cdt.org/legislation/105th/privacy/coppa.html

[211] Ver definición de página *web* en nota 83.

[212] Texto completo de la ***Aviation and Transportation Security Act***, Transportation and Security Administration (TSA), http://www.tsa.gov/research/laws/law_regulation_rule_0010.shtm

como el nombre, la nacionalidad, el sexo, pasaporte, visa y lo que denomina esta ley "cualquier información necesaria para garantizar la seguridad aérea", nos relata Rocío Ovilla: "no se conformaron con estos datos (los ya señalados) y pidieron de las compañías que les permitieran el acceso a sus sistemas de reservación, en el cual pueden existir información altamente confidenciales sobre los pasajeros. Esta obligación se realizó mediante la aprobación de una reglamentación del 25 de junio de 2002 llamada *Passanger Name Record*, PNR."[213]

Esta medida sitúa a las aerolíneas que operan en la Unión Europea entre la espada y la pared. Si no proporcionan a las autoridades estadounidenses acceso a los PNR[214], pueden ser sancionadas con multas millonarias e incluso pérdida de los derechos de vuelo a los Estados Unidos. Por otra parte, las leyes de protección de datos de los Estados miembros de la UE (la ya mencionada Directiva europea 95/46) establecen requisitos estrictos para la transferencia internacional de datos personales, incompatibles con el nuevo sistema estadounidense de control previo de pasajeros. En consecuencia, si las compañías europeas acceden a las exigencias estadounidenses, ellas y sus ejecutivos pueden ser sancionados con multas millonarias por las agencias nacionales de protección de datos.

Con el fin de encontrar una solución a este conflicto de leyes y de intereses nacionales -la seguridad estadounidense frente a las libertades individuales y la protección de datos personales en la Unión Europea-, la Comisión europea entabló contactos bilaterales. Las negociaciones se intensificaron a finales de 2002 y las autoridades estadounidenses consintieron en posponer la entrada en vigor efectiva de la medida hasta el 5 de marzo de 2003. El objetivo último de la Comisión era y sigue siendo la obtención de garantías respecto al funcionamiento y aplicación del nuevo sistema de control de pasajeros que le permitan adoptar una decisión considerando el sistema compatible con la Directiva Europea 95/46. Dicha solución evitaría la intervención de las agencias nacionales de protección de datos con el consiguiente riesgo de soluciones divergentes, conflictos con las autoridades estadounidenses y, en última instancia, perjuicios para las compañías y los pasajeros europeos.

A comienzos de 2003 la posibilidad de un conflicto político y comercial de grandes proporciones adquiría cada vez más fuerza y el Parlamento Europeo fijó su atención en esta cuestión, requiriendo a la Comisión una actuación concertada. Sin embargo, poco después la Comisión y las autoridades estadounidenses emitieron una declaración conjunta anunciando una serie de compromisos transitorios en forma de mayores (pero aún insuficientes) garantías respecto al acceso a los PNR y su voluntad común de llegar a una solución definitiva mediante una decisión en virtud del artículo 25.6 de la Directiva 95/46 o un acuerdo bilateral entre la UE y EE UU. Esta declaración no

---

[213] BUENO OVILLA, Rocío, ***La protección de los datos personales en México***, Editorial Porrúa, México, 2005, colección Breviarios Jurídicos No. 28, pág. 22.

[214] Este PNR puede contener informaciones sobre el lugar en donde se hizo la reservación, el número de persona que hicieron la reservación, el medio de pago, la dirección personal del pasajero, número telefónico, si reservó un hotel o un automóvil, la comida pedida y los servicios relativos a la salud.

tenía efectos jurídicos, pero invitaba a las agencias nacionales de protección de datos a no actuar contra las empresas que proporcionasen a las autoridades estadounidenses acceso a sus PNR, mientras continuaban las negociaciones. Ello motivó una reacción airada del Parlamento Europeo por no haber sido consultado en este proceso, considerando una claudicación de la Comisión frente a los intereses estadounidenses.

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 en el resto del mundo, en especial de las europeas como es notorio con la entrada en vigor de la *Aviation and Transportation Security Act.*

B) Canadá

a) Normas constitucionales

De un análisis exhaustivo a la Constitución de Canadá[215] no encontramos normas que protejan específicamente el derecho a la vida privada de las personas, menos sobre la protección de datos personales, al igual que el Reino Unido, de donde es descendiente la mayor parte de su familia jurídica, la del *common law.*[216] En cambio dentro de su prolífica legislación interna federal e incluso local vamos a encontrar normas que regulan de manera concreta la protección de estos derechos, por el alcance que persigue este trabajo no vamos a hacer un estudio detallado de cada provincia y menos aun de su abundante producción jurisprudencial en la materia.

b) Normas Internas

Canadá tiene dos leyes federales que tratan sobre la privacidad, por una parte el *Privacy Act* y el *Personal Information and Electronics Documents Act.*

El *Privacy Act* o Ley de Privacidad, fue aprobado el 1 de julio de 1983. Esta Ley impone obligaciones en más de 150 departamentos y agencias del gobierno federal para respetar los derechos de privacidad y limitar la recolección, uso y disposición de datos personales. La Ley de Privacidad también le da a los ciudadanos el derecho a acceder y pedir la corrección de sus datos personales

---

[215] Texto completo en ***The Solon Law Archive***, http://www.solon.org/Constitutions/Canada/English/ca_1982.html

[216] Entendemos por *common law*, al "sistema jurídico anglo-norteamericano, dentro del sistema jurídico anglo-norteamericano, el conjunto de reglas y normas tradicionales que constituyen el núcleo común de los Derechos de este sistema, particularmente según han sido reconocidos por la jurisprudencia, en una acepción más amplia que la anterior, siempre dentro del sistema jurídico anglo-norteamericano, las normas y reglas que no tienen origen legislativo" CABANELLAS DE LAS CUEVAS Guillermo y C.HOAGUE, Eleanor, ***Law Dictionary***, Tomo 1 English-Spanish, Editorial Heliasta, Buenos Aires, Argentina 1998, pág. 151. Para más referencias sobre el common law, ver la obra de ZWEIGERT, Konrad y KÖTZ, Hein, ***Introducción al Estudio del Derecho Comparado***, Oxford Universty Press, México, 2002, págs 193-252.

que posean las organizaciones del gobierno federal. Así su numeral segundo dice a la letra:

> 2. Propósito. El propósito de esta Ley es extender la protección de esta a todas las leyes de Canadá con el fin de proteger la privacidad de los individuos en relación a la información personal que este en posesión de cualquier institución de gobierno y proveer a los ciudadanos el derecho de acceder a dicha información. [217]

En segundo lugar los ciudadanos canadienses están protegidos por la *Personal Information Protection and Electronic Documents Act* (PIPEDA), del 13 de abril de 2000 y sus reformas del 3 de marzo de 2006, que contiene entre otras disposiciones, los estándares mínimos de protección a la vida privada en el ámbito del sector privado. Establece las reglas de cómo se recolecta, utiliza o se dispone de los datos personales recolectados por empresas y su utilización en actividades comerciales, también da el acceso a la revisión, corrección de los datos personales que estas organizaciones hayan recolectado.

> **Aplicación: 1)** Esta ley es aplicable a toda organización que recolecte información personal y tiene el fin de proteger los datos personales en los siguientes sentidos:
>
> a) La organización que recolecte, use, disponga de dichos datos personales con fines comerciales; o
>
> b) Información que sea de un empleado de la organización del cual la misma haya obtenido, utilice o disponga en conexión con alguna otra información que tenga que ver con un trabajo federal o que no este dentro de su ámbito de de actividades.[218]

Si una ley sobre privacidad de alguna provincia canadiense no cumple con los requisitos del PIPEDA, el gobierno federal podría desconocer dicha ley y no considerarla como "substancialmente similar".

A nivel internacional el PIPEDA fue una de las primeras leyes reconocidas por el Parlamento y el Consejo de la Unión Europeas como suficientemente "adecuada" para propósitos comerciales, después de su promulgación tuvo una entrada en vigor en tres fases, la primera entro en vigor desde el primero de enero del 2001 y aplica a la regulación de organismos federales, específicamente a la información personal que utilicen organismos en actividades comerciales, así como información que las organizaciones recolecten utilicen o proporcionen sobre sus empleados en relación con actividades laborales, de compromiso o de negocios a nivel federal, el 1º de enero de 2002 entro en vigor la segunda fase, que regula la información sobre salud de los individuos, la tercera fase entro en vigor el 1º de enero de 2004 y regula a organizaciones bajo la jurisdicción de cada una de las provincias

---

[217] Artículo 2 de la *Privacy Act*, ***Department of Justice Canada***, http://laws.justice.gc.ca/en/P-21/Index.html

[218] Artículo 1 de la *Personal Information Protection and Electronic Documents Act*, ***Department of Justice Canada***, http://laws.justice.gc.ca/en/P-8.6/258031.html

canadienses, a menos que cada provincia implemente una legislación especifica para el sector privado substancialmente similar al PIPEDA.

Podemos decir que Canadá ha seguido políticas de regulación sobre privacidad y protección de datos que se han caracterizado por la adopción de la llamada "*thrid way*" o tercera vía, es decir han tratado de adoptar un marco regulatorio que no sea ni excesivamente sobre regulado por el gobierno ni tampoco que sea libremente autorregulado por las empresas, sino que combine legislación y políticas de autorregulación eficientes que respondan a los derechos de los ciudadanos y consumidores, estableciendo reglas claras y organismos gubernamentales adecuados.[219]

3.- 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".[220]

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* impropio). La primera de ellas, generalmente 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".[221]

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

---

[219] Por ejemplo en Canadá se cuenta con la ***Office of the Privacy Commissioner of Canada***, que tiene como principal objetivo el promover y proteger los derechos de privacidad de los ciudadanos, así como velar por el cumplimiento y aplicación de la legislación en la materia. Esta es la dirección de su sitio en Internet: http://www.privcom.gc.ca/

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

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

jurídico al ya mencionado habeas data, que en general tienen un desarrollo bastante más precarios que el de los países reclén estudiados.

A) Brasil

a) Normas constitucionales

La Constitución Federal del Brasil, promulgada en el año de 1998, protege constitucionalmente el derecho a la vida privada de sus ciudadanos. Tal protección se encuentra consagrada en lo 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".[222]

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;[223]
> b) para rectificar datos, cuando no de prefiera hacerlo por procedimiento secreto, judicial o administrativo".[224]

b) Normas internas

Si bien la Constitución Brasileña 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 reclén 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

---

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

[223] Artículo 5, LXXII de la Constitución de la República de Brasil. Dentro de la doctrina brasileña, 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 PUCCINELLI, Oscar, ***El Habeas Data en Indoiberoamérica***, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1999, pág. 307.

[224] Constitución de la República Federativa de Brasil. ***Cámara de Diputados de la República Federativa de Brasil***, http://www2.camara.gov.br/legislacao/constituicaofederal.html

de *habeas data*". Así, el artículo séptimo de dicha ley señala los casos en que procede este remedio constitucional:

> "Artículo 7. Concédase 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 atención en los asientos del interesado, de contestación o explicación sobre datos verdaderos pero justificables y que estén en dependencia judicial o amigable".[225]

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 puede 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".[226]

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 propósito no autorizados por ley constituye delito".[227]

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 brasileña en cuanto a la protección de la correspondencia en el ámbito laboral entre trabajadores y empleadores.

B) Ecuador.

a) Normas 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:

---

[225] Artículo 7 de la ***Ley 9.507*** de 12 de noviembre de 1997 que regula el Recurso de *Habeas Data* en Brasil. Cámara de Diputados de la República Federativa de Brasil, http://www2.camara.gov.br/legislacao/produtos/leginfra/conteudo

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

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

"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 en 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."[228]

Unos 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 tiene protección de rango constitucional.

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 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.

---

[228] Artículos 8 y 13 de la Constitución Política de la República del Ecuador, ***Gobierno Nacional de la República de Ecuador***, http://www.presidencia.gov.ec/modulos.asp?id=109

> La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional".[229]

b) 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".[230]

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 Pesantez, "el defensor del pueblo está 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*".[231]

En cuanto a la protección del derecho a la vida privada en Internet la "Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos", establece que:

> "Artículo 9 (segundo párrafo).- La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.
>
> "Disposiciones generales.
> Novena.- Glosario de términos.
> Intimidad: El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta Ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no

---

[229] Artículo 94 de la Constitución Política de la República del Ecuador, ***Gobierno Nacional de la República de Ecuador***, http://www.presidencia.gov.ec/modulos.asp?id=109

[230] Artículo 34 de la Ley de Control Constitucional, ***Comisión Andina de Juristas***, http://www.cajpe.org.pe/RIJ/bases/legisla/ecuador/lh-25.HTMI

[231] SALGADO PESANTEZ, Hernán, ***Lecciones de Derecho Constitucional***, Ediciones Legales, Quito, Ecuador, 2004, pág. 118.

> divulgación de los datos personales y a no recibir información o mensajes no solicitados.[232]

Es particularmente destacable esta 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*, 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.

C) Argentina

a) Normas constitucionales

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.[233]

> "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". [234]

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"[235] 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.

b) Normas internas

---

[232] Artículo 9 y Novena Disposición General de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, ***Consejo Nacional de Telecomunicaciones de Ecuador***, http://www.conatel.gov.ec/website/baselegal/leyes.php?nomb_grupo=leyes&cod_nivel=n1&cod_cont=23

[233] 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.

[234] Artículo 43 de la Constitución Federal de la República Argentina, ***Honorable Senado de la Nación***, http://www.senado.gov.ar/web/interes/constitucion/capitulo2.php

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

A nivel latinoamericano, una de las leyes que encontró mas trabas para ser promulgada es la Ley 25.326 o Ley de Protección de los Datos Personales del año 2000.[236] 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 1° 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.
> 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".[237]

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 mismo, 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".[238]

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 artículo21.

---

[236] Es preciso señalar que en 1996, el Congreso de la Nación aprobó la Ley 24.745, regulatoria del *habeas 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.

[237] Artículo primero de la Ley 25.326 de Protección de los Datos Personales de la República Argentina, aprobada en 2000, http://www.proteccíondedatos.com.ar/ley25326.htm

[238] Artículo 12 de la Ley 25.326 de Protección de los Datos Personales de la República Argentina, aprobada en 2000, http://www.proteccíondedatos.com.ar/ley25326.htm

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 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 asemejan 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 usuario de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el 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.- Dicho 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".[239]

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 *emails* 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 *emails* basándose en una interpretación extensiva de un artículo del Código Penal argentino que protege la privacidad de los secretos".[240]

---

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

[240] ROSEMBERG HOLCBLAT, Alexander y SÁNCHEZ SANZ, Moriah, ***El derecho a la privacidad en Internet***, Revista de Derecho Informático, No.37, Agosto de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=770

CAPÍTULO TERCERO

LA PROTECCIÓN DEL DERECHO A LA VIDA PRIVADA EN EL ORDENAMIENTO JURÍDICO MEXICANO

"Hay que armonizar el interés público a la información con el interés privado a la intimidad."
Jorge Carpizo y Alonso Gómez – Robledo Verduzco

CAPÍTULO TERCERO. LA PROTECCIÓN DEL DERECHO A LA VIDA PRIVADA EN EL ORDENAMIENTO JURÍDICO MEXICANO

El derecho a la vida privada 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 garantías. El ordenamiento jurídico mexicano no ha sido la excepción, y es así que el derecho a la vida privada de las personas ha encontrado un reconocimiento que cabe decir, no ha logrado ser expreso tanto a nivel constitucional como al nivel de otras normas de distinto rango.

A través del presente capítulo haré un breve análisis del reconocimiento jurídico que el sistema mexicano ha dado a la protección del derecho a la privacidad de las personas, partiendo de las normas constitucionales, para después continuar con las leyes federales y finalmente proyectos de ley que actualmente se encuentran en trámite en el Congreso de la Unión. 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, o resultan todavía insuficientes en distintos ámbitos y en distintos campos, como se verá a continuación.

I.- Constitución Política de los Estados Unidos Mexicanos

Existen voces dentro de la doctrina nacional en el sentido de afirmar que la protección a la vida privada no puede ser configurado como un derecho fundamental, postura de la que difiero diametralmente y para lo cual presento varios argumentos que sostienen mi tesis de afirmar que si bien no existe una mención expresa en nuestra Carta Magna que consagre la protección de la vida privada en Internet, si podemos inferir que de una interpretación armónica que dicha protección existe, aunque muy incipiente, lo cual requiere de una inclusión en la Constitución para lo cual tratamos de justificar dicha postura desde un punto de vista garantista.

1.- La protección de datos personales como derecho fundamental

Es necesario primero definir lo que es un derecho fundamental, trataremos entonces de dar una aproximación al mismo. El maestro Miguel Carbonell, en su excelente obra "Los derechos fundamentales en México" nos dice textualmente: "considerando la pluralidad de conceptos y definiciones que existen de los derechos fundamentales, quizá la mejor sea ofrecer solamente la que nos permita comprender después el significado de los derechos dentro del sistema jurídico mexicano. Una de las mejores definiciones que se han realizado de los

derechos fundamentales es la de Luigi Ferrajoli."[241] Ahora bien, es preciso dedicar unas cuantas líneas a la construcción teórica de Ferrajoli.

El hilo conductor es muy claro, la limitación del poder, para lograr dicho fin, busca elaborar una teoría que aborde el tema desde lo jurídico, sin dejar de ser multidisciplinaria, la que ha denominado "teoría general del garantismo", la cual abre la posibilidad de resolver los principales problemas de la legitimación, legalidad, existencia, vigencia, validez y efectividad del derecho, utilizando sus propias herramientas metodológicas.

En primer término, su metodología es un ambicioso proyecto con dos ramificaciones, que en principio parecen contradictorias: una teoría de la justicia política (por utilizar la expresión de Höffe) y una teoría pura del derecho (en uso de la sentencia de Kelsen). En otras palabras, intenta, por un lado, conciliar dos formas de pensamiento distintos: el iusnaturalismo y el iuspositivismo; y, por el otro, superar las deficiencias en que aquellos reduccionismos han incurrido. En segundo término, sus presupuestos filosóficos son tan variados como su metodología. Punto de partida es la firme adhesión a la razón y su simpatía a la filosofía kantiana. Además de agregar a su escarcela consistentes dosis de filosofía analítica, socialismo y de realismo jurídico. Por otra parte, aunque sería difícil catalogarlo como hobbesiano, Ferrajoli acude reiteradamente a la obra del político inglés. Heredero de la tradición contractualista, deposita su armazón en el pensamiento político hobbesiano y considera que para minimizar la violencia interpersonal dentro de las sociedades es necesario un Estado de derecho, cuya herramienta principal es el orden jurídico "el cual, por lo mismo, se configura, al menos en la edad moderna, como una técnica dirigida a limitar, disciplinar y, por consiguiente, minimizar el poder"[242]. (No obstante, y considerando que Hobbes es un representante de la idea de un gobierno de los hombres[243], se aleja de la fuente de su inspiración cuando enfatiza que busca un gobierno de las leyes y no un gobierno de los hombres).

El punto de partida, como hemos mencionado, es el poder. En una aseveración bastante ejemplar de su pensamiento manifiesta que "El poder — todos los poderes, sean estos públicos o privados— tiende en efecto, ineludiblemente, a acumularse en forma absoluta y a liberarse del derecho"[244].

Para concretizar su forma de limitar al poder, primero, elabora su propia tipología de los poderes. Así, establece dos clasificaciones básicas de cuya intercesión resultan, al final, cuatro variantes. Son relaciones básicas las

---

[241] CARBONELL, Miguel, ***Los derechos fundamentales en México***, Instituto de Investigaciones Jurídicas, UNAM, México, 2004, pág. 12.

[242]FERRAJOLI, Luigi, ***El garantismo y la filosofía del derecho***, Universidad externado de Colombia, Bogotá, 2000, pág. 122

[243] El profesor Gregorio Peces-Barba escribe que "La supremacía del poder sobre el Derecho es la del gobierno de los hombres sobre el gobierno de las leyes... En la cultura jurídica moderna una corriente teórica que arranca de Bodino y de su definición de la soberanía, que sigue con Hobbes o con Spinoza y que tiene su máxima expresión moderna con Carl Schmitt, representa esa idea de la supremacía del poder sobre el derecho" PECES-BARBA, G. ***Curso de derechos Fundamentales. Teoría general.*** BOE, Madrid, 1999, pág. 324.

[244]FERRAJOLI, L. Op. cit. pág. 121

siguientes: 1) poderes salvajes ilegales (contra el derecho) y los poderes salvajes extralegales (fuera del derecho); 2) poderes de la sociedad (privados) y poderes del estado (públicos). Interrelacionando surgen cuatro clases: a) poderes privados ilegales; b) poderes públicos ilegales; c) poderes privados de tipo extralegal y d) poderes públicos extralegales[245]. Ejemplifico, de manera propia cada clasificación. Un ejemplo de la primera clasificación —poderes privados ilegales— lo es el poder de las organizaciones de narcotráfico en el caso de México y Colombia. Para un modelo de la segunda —poderes públicos ilegales— podemos acudir para su representación a la organización policial y secreta rusa del año de 1881 llamada OJRANA. Por lo que se refiere a la tercera —poderes privados de tipo extralegal— un modelo aplicable es el de la situación de los trabajadores inmigrantes mexicanos en Estados Unidos que, debido a la falta de garantías especificas de protección, el abuso en nombre del "libre mercado", permite la explotación en las esferas privadas y fuera del derecho. Finalmente, para ejemplificar la cuarta clasificación —poderes públicos extralegales— tenemos que acudir a dos ejemplos. Esto se debe a que Ferrajoli distingue los poderes públicos extralegales internos y los poderes públicos extralegales externos. Los poderes públicos extralegales internos se pueden ejemplificar con el caso de los nombramientos de los jueces naturales.[246] Por otra parte, los de carácter externo, se realizan en las situaciones del derecho internacional. A decir de Ferrajoli, el derecho internacional ante la carencia de garantías efectivas de protección y de limitación del poder en el ámbito internacional, se cometen de forma permanente abusos de poder en el plano internacional como en el caso de la guerra del Golfo, el terrorismo y los Balcanes.

Para Ferrajoli, El Estado de derecho garantista, se ofrece como la mejor alternativa para la limitación de esos poderes. Estado de derecho garantista que exige dos cosas: una concepción propia de la teoría del derecho y una filosofía política. Requiere de una exclusiva visión de la teoría del derecho debido a que el Estado garantista cambia el paradigma clásico del derecho por una alternativa distinta y crucial para las exigencias de las sociedades actuales. Por otra parte, necesita de la re-elaboración de una filosofía política particular que atienda la demanda de la nueva relación entre política y derecho. En otras palabras, —y de ahí se desprenden sus tres acepciones de garantismo— Ferrajoli pretende elaborar una teoría general del garantismo con visiones propias del Estado de derecho, teoría del derecho y filosofía política.

Después de esta breve referencia a la teoría garantista, es preciso dar la definición de Ferrajoli sobre lo que el denomino *Diritti fondamentali*: "todos aquellos derechos subjetivos que corresponden universalmente a todos los seres humanos en cuanto dotados de status de personas, de ciudadanos o de personas con capacidad de obrar".[247] En este orden de ideas, considero que la vida privada es un derecho subjetivo que corresponde a todos los seres

[245] Idem, 126-131.

[246] Recordemos que en un momento histórico y en ciertos países (como sucedió en Costa Rica con los tribunales especiales del periodo post-revolucionario del año de 1948) se instituían jueces o tribunales, ante la falta de reglamentación especifica, para un caso concreto (principio del juez natural).

[247] FERRAJOLI, Luigi, ***Derechos y garantías. La ley del más débil,*** Editorial Trotta, Madrid, 2004, pág. 37.

humanos, de esta manera podemos decir que existen derechos fundamentales consagrados en nuestra Constitución Política, como dijera Carbonell, "podríamos decir que todos los derechos fundamentales son derechos humanos *constitucionalizados*".[248]

Por lo tanto, lo que procede es señalar el porque de la importancia de constitucionalizar la protección de datos personales. Siguiendo de nueva cuenta a Carbonell: "La mejor doctrina sobre el tema (Ronald Dworkin, Luigi Ferrajoli, Ernesto Garzón, etcétera) parece estar de acuerdo en que la constitucionalización de un derecho supone, entre otras cuestiones, poner una determinada expectativa a un bien jurídico fuera del alcance del mercado y de la política ordinaria. Supone, por tanto, dejar a salvo de las fuerzas del dinero y de los intereses políticos determinado tipo de bienes, como dijera el experto en Derecho Informático, Julio Téllez: "La capacidad de almacenamiento, tratamiento, transmisión y uso de información como elemento fundamental para la toma de decisiones en aspectos económicos por parte de personas e instituciones tanto en el sector público como en el privado, llegan a ser equiparadas con elementos como la energía y las materias primas. La importancia económica de la información no está puesta en duda, es un verdadero bien susceptible de apoderamiento con un innegable valor patrimonial o contenido económico inherente que radica en el destino o utilidad de la misma."[249] La clave para lograr lo que se acaba de decir encuentra en el carácter de universal de los derechos fundamentales, tal como lo ha puesto en evidencia el concepto que propone Luigi Ferrajoli."[250] De esta manera podemos afirmar que si se le da el grado de derecho fundamental a la protección de datos personales, los mismos quedarían fuera del alcance de esas fuerzas del dinero (la libre empresa) y la política ordinaria (el caso *Choicepoint* entre otros), para tener una protección amplia y un recurso jurisdiccional para hacer valer tal derecho.

Como refuerzo a lo ya mencionado es importante destacar lo que ha sucedido en la doctrina internacional para la configuración de la protección de datos como un derecho fundamental, podemos decir que existe un desarrollo en la doctrina y en las normas acerca de este derecho. Al menos la Unión Europea lo considera un derecho fundamental. Al decir de Agustín Puente Escobar:[251] "... a diferencia de lo acontecido con otros derechos fundamentales cuyo desarrollo se produjo paralelamente en el ámbito de Europa y de los Estados Unidos, el derecho a la protección de datos de carácter personal tiene un origen marcadamente europeo, ya que el desarrollo de las primeras legislaciones de protección de datos tiene lugar en Europa."

---

[248] CARBONELL, Miguel, ***Los derechos fundamentales en México***, Instituto de Investigaciones Jurídicas, UNAM, México, 2004, pág. 9. Cabe señalar que el maestro Carbonell realiza una excelente distinción entre derechos humanos, garantías individuales y derechos fundamentales, siendo amplio este estudio y poco el espacio para tratarlo, llegando a la conclusión que hemos citado, como corolario de que existe una estrecha relación entre las tres definiciones.

[249] TELLEZ VALDEZ, Julio, ***Derecho Informático***, McGraw – Hill, México, 2004, págs. 59-60.

[250] CARBONELL, Miguel, ***El derecho de acceso a la información como derecho fundamental*** en LÓPEZ-AYLLÓN, Sergio (coord.), ***Democracia, transparencia y Constitución: propuestas para un debate necesario***, México, UNAM, Instituto de Investigaciones Jurídicas, 2006, pág. 10.

[251] PUENTE ESCOBAR, Agustín, "Breve descripción de la evolución histórica del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal", ***Protección de datos de carácter personal en Iberoamérica***, Agencia Española de Protección de Datos, 2005, pág. 39.

Así las cosas podemos destacar la forma de regulación que se ha dado en Europa y que hemos tratado en nuestro estudio de derecho comparado, por lo que no seremos profundos en su estudio. Es el caso de la Constitución española de 1978, que dentro del apartado relativo a los derechos fundamentales, se reconoce en el artículo 18.4, que la ley limitará el uso de la informática para garantizar la intimidad personal y familiar de los ciudadanos. Esto aun no nos habla de un derecho fundamental de protección de los datos personales, fue finalmente con el pronunciamiento del Alto Tribunal español en sus sentencias 290/2000 y 292/2000 de 30 de Noviembre ambas, cuando se produce la consagración del derecho fundamental a la protección de datos personales, esto es, "el derecho a la libertad informática". Dentro de sus fundamentos jurídicos 6 y 7 cuando finalmente establece el reconocimiento de un nuevo derecho. En el primero de estos se puede leer lo siguiente:

> El derecho fundamental a la protección de datos persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho del afectado...
>
> El objeto de protección del derecho fundamental de la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el artículo 18.1 de la C.E. otorga, sino los datos de carácter personal.

Por su parte, el Fundamento Jurídico 7 se pronuncia acerca del contenido de la protección de datos personales disponiendo lo siguiente:

> El contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuales de estos datos proporcionar a un tercero, sea el Estado o un particular.[252]

De esta forma podemos decir que en España se ha configurado el reconocimiento al derecho fundamental de la protección de datos.

Debe quedar muy bien asentado que la protección de datos personales es un derecho fundamental independiente del derecho a la intimidad como se ha visto en Europa. El decidir cuándo, como y quien va a tratar la información personal, es un derecho que tiene todo individuo, como ya hemos dicho, sin reconocimiento constitucional en nuestro país, esto significa que se debe implementar el enunciado expreso de un derecho fundamental dentro de la ley suprema mexicana, como es la protección de datos personales. En este capítulo hemos de tratar las iniciativas que se han planteado para la promulgación de una ley de protección de datos personales, pero antes debemos estudiar la

[252] Sentencia que tiene como antecedentes una serie de recursos -201/1993, 226/1993 y 236/1993- interpuestos por el Consejo Ejecutivo de la Generalidad de Cataluña, el Defensor del Pueblo, el Parlamento de Cataluña y 56 Diputados contra determinados artículos de la Ley 5/1992 de 29 de Octubre, de Regulación el Tratamiento Automatizado de Datos de Carácter Personal.

materia constitucional, por lo tanto debemos mencionar dos iniciativas con proyectos de reforma a la Constitución para incluir el derecho fundamental de la protección de datos en nuestro ordenamiento máximo. Siguiendo a Robert Alexi[253] debemos decir que como derecho fundamental el de la protección de datos personales debe tener las características de todo derecho de esta categoría: máximo rango, máxima fuerza jurídica y máxima importancia del objeto y máximo grado de indeterminación, ubicándose así en la cúspide de los derechos tutelados por el ordenamiento, de esta forma se aportaran los elementos para que en la legislación secundaria y en los actos del poder público y particulares, existan vías jurídicas idóneas que protejan de manera efectiva este derecho en la realidad social.

Aun más lejos en el IV Encuentro Iberoamericano de Protección de Datos Personales celebrado en México del 2 al 4 de noviembre de 2005, se redactó lo que se dio por denominar la "Declaración de México",[254] que en su apartado I contempla: "El derecho fundamental de la protección de los datos personales": "El derecho a la protección de datos personales presenta caracteres propios que le dotan de una naturaleza autónoma de tal forma que su contenido esencial le distingue de otros derechos fundamentales y, específicamente, del derecho a la intimidad, al honor y a la propia imagen. El derecho a la protección de datos atribuye a la persona un poder de disposición y control sobre los datos que le conciernen, partiendo del reconocimiento de que tales datos van a ser objeto de tratamiento por responsables públicos y privados. Dicho tratamiento impone a los responsables una obligación positiva al objeto de que se lleve a cabo con pleno respeto al sistema de garantías propio de este derecho fundamental." Y nos dice que únicamente de esta forma podremos alcanzar un marco de respeto adecuado al respeto de este derecho fundamental: "Sin embargo, no puede olvidarse que sólo respetando el derecho fundamental de todos a la protección de sus datos personales se conseguirá un marco adecuado de respeto a la libertad de expresión, al acceso a la información y un correcto desarrollo del mercado."

Para concluir Celis Quintal[255] nos relata de forma amplia la justificación del porque debe de ser incorporado el derecho de protección de la vida privada en la Constitución de nuestro país: "El sistema jurídico mexicano tiene un déficit normativo en lo que se refiere a la protección de la vida íntima de los mexicanos. En la Constitución no se reconoce el derecho a la intimidad como fundamental, y se regula parcialmente como derivación de la tutela de otros derechos fundamentales, como la inviolabilidad de las comunicaciones privadas y la limitación a la libertad de imprenta." Así continua diciendo que esto origina carencias entre las que figuran principalmente: "La falta de reconocimiento expreso en la Constitución federal del derecho a la intimidad como un derecho

---

[253] ALEXI, Robert, ***"Los derechos fundamentales en el Estado democrático de derecho"***, en ***Neoconstitucionalismo (s)***, CARBONELL, Miguel (ed.), Madrid, Trotta, 2003, págs. 32 y 33.

[254] ***Declaración de México***, IV Encuentro Iberoamericano de Protección de Datos Personales, México, 2 al 4 de Noviembre de 2005, Agencia Española de Protección de Datos, https://www.agpd.es/index.php?idSeccion=525

[255] CELIS QUINTAL, Marcos Alejandro, ***La protección de la intimidad como derecho fundamental de los mexicanos*** en ***Estudios en Homenaje a Marcia Muñoz de Alba Medrano. Protección de la persona y derechos fundamentales***, CIENFUEGOS SALGADO, David y MACIAS VAZQUEZ, María del Carmen (coords.) Instituto de Investigaciones Jurídicas, UNAM, México, 2006, pág. 101.

fundamental de los mexicanos, y la carencia de una protección integral de ese derecho; La falta de protección contra la obtención de documentación o información que pueda ser usada en juicio contra los individuos; "la falta de protección de los datos personales, como los antecedentes médicos o genéticos."

Podemos decir que el reconocimiento de la vida privada en la Constitución haría procedente el juicio de amparo en contra de actos de autoridad que violen el derecho a la vida privada de las personas y con ello conseguir la interrupción de las violaciones mediante la suspensión del acto reclamado. La experiencia de otros países como España, Alemania, Argentina o los Estados Unidos demuestran el funcionamiento que tiene este reconocimiento, limitando así los excesos de los factores de poder, como lo son los medios de comunicación o las empresas.

2.- Iniciativas de reforma a la Constitución Federal, para incluir el derecho fundamental de la protección de datos personales.

A) Iniciativa de adición al artículo 16 de la Constitución presentada por el Senador Antonio García Torres de 21 de febrero de 2001.

Esta iniciativa fue publicada en la Gaceta Parlamentaria del 21 de febrero de 2001[256] y propone la adición de tres párrafos al artículo 16 de nuestra Carta Magna:

> "Toda persona tiene derecho a la **protección y al acceso de los datos personales que le conciernen**, así como el de acceder a la información de archivos o registros públicos y privados destinados a dar informes, y a conocer el uso o finalidad de tales registros. Los datos se obtendrán y tratarán de modo que no se afecten el honor, la intimidad o cualquier otro derecho de las personas, para fin lícito determinado y con el previo consentimiento, libre e informado de su titular.
>
> No se considera que la obtención y el tratamiento de datos afecta el honor, la intimidad o cualquier otra garantía de la persona a la que conciernen, cuando se realizan atendiendo al interés general del Estado mexicano, a intereses sociales, o con el fin de proteger los derechos fundamentales de terceros por causa legítima.
>
> La persona tiene derecho a la inclusión, actualización, complementación, rectificación, suspensión, reserva y cancelación de los datos que le conciernen."

En la exposición de motivos señala varias referencias legislativas internacionales como tratados y legislación de otros países, realizando una narración cronológica de cómo se ha venido desarrollando este derecho, señala expresamente: "Este derecho, implícitamente reconocido en la Constitución Política de los Estados Unidos Mexicanos, en su artículo 16, se encuentra en constante riesgo ante el avance de las nuevas tecnologías, fundamentalmente

---

[256] ***Gaceta Parlamentaria, año IV, número 692***, Cámara de Diputados, México, D.F., miércoles 21 de febrero de 2001, http://gaceta.diputados.gob.mx/Gaceta/58/2001/feb/20010221.html#Ini20010221Antonio

de la información que, ahora, tienen la potencialidad de colectar, tratar y comunicar o difundir en tiempos, formas y condiciones prontas, rápidas e, incluso, automáticas, la información atinente a una persona, con riesgo de lesionar sus derechos fundamentales, cualquiera que estos sean, y de manera especial, los derechos a la intimidad subyacentes en el supramencionado artículo 16 constitucional." De lo anterior notamos que se hace referencia a un reconocimiento implícito de este derecho, pero no explícito por lo tanto la propuesta de adición.

La suerte de la misma no fue muy afortunada, ya que se turnó a las Comisiones de Puntos Constitucionales y de Estudios Legislativos de la Cámara de Senadores. El día 4 de abril del 2006 la iniciativa fue votada dispensando la segunda lectura, sin embargo no logró los votos necesarios de mayoría calificada, por lo que el dictamen fue desechado.

B) Iniciativa de adición al artículo 16 de la Constitución presentada por el Senador Antonio García Torres el 5 de abril de 2006.

De esta forma el día 5 de abril de 2006 el Senador García Torres presenta esta nueva iniciativa de adición que en su parte expositiva contiene mejores argumentos y un renovado enfoque de garantismo que no se había notado en su propuesta anterior y así en su punto segundo señala lo que sigue:

> "SEGUNDO.- Lo que esta iniciativa propone es que la Constitución reconozca, en el artículo 16 la protección de los datos personales como un derecho fundamental, con el fin de darle estabilidad, eficacia y seguridad, puesto que la Constitución sólo prevé el derecho a la intimidad y privacidad, personal y familiar y el derecho al honor.
>
> El derecho a la protección de los datos personales ha sido confundido con los derechos a la intimidad-privacidad y el honor, cuando en realidad es un derecho nuevo.
>
> Por esa razón resulta necesario y útil distinguir entre los diferentes derechos próximos entre sí al derecho de protección de datos personales, esto es, frente a los derechos a la intimidad-privacidad, al honor y la imagen.
>
> Una muestra clara de que el derecho a la protección de datos personales es un derecho fundamental autónomo y distinto de los derechos al honor, la imagen y la privacidad lo constituye el artículo 8 de la Carta de los Derechos Fundamentales de la Comunidad Europea..."[257]

Notamos entonces como se hace el planteamiento de que sea reconocido como "derecho fundamental" la protección de datos personales, destacando que nuestra carta magna solo protege derechos de intimidad, privacidad u honor, para fortalecer lo anterior es oportuno señalar lo que dice la primer consideración del Dictamen de las Comisiones unidas de Puntos Constitucionales y Estudios Legislativos, el que contiene el proyecto de decreto

---

[257] ***Gaceta del Senado, No.164, Año 2006***, México, D.F., miércoles 5 de abril de 2006, Senado de la República, http://www.senado.gob.mx/sgsp/gaceta/index2.php?sesion=2006/04/05/1&documento=9

por el cual se adicionan dos párrafos al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos:

> **Primera**. Las Comisiones dictaminadoras consideran que la iniciativa de adición constitucional debe aprobarse, en sus términos.
>
> Los derechos fundamentales tienen un basamento justificativo en tres diversos órdenes: filosófico-axiológico, histórico y sociológico.
>
> Por una parte, se puede considerar que los derechos fundamentales constituyen en sí mismos o tutelan bienes y valores fundamentales del ser humano, sin los cuales el ser humano no se podría concebir como tal. Por ejemplo, hoy es impensable la existencia del ser humano sin el reconocimiento de su derecho a la libertad, hoy no podemos considerar la existencia del hombre esclavo, sobre todo en los términos del liberalismo clásico.
>
> Por otra parte, si bien los derechos humanos fundamentales tienen un contenido filosófico-axiológico, ético en suma; se debe reconocer que el proceso de reconocimiento de los derechos fundamentales ha corrido por los diversos hitos de la historia, en el que juegan un papel clave la Magna Carta de Juan sin Tierra de 1215, la Constitución Americana de 1776 (sic)[258], y la Declaración *francesa* de los Derechos y Deberes del Hombre de 1789-subsecuentemente modificada-, como bien se señala en la iniciativa.
>
> En ese desarrollo histórico, también debe recordarse la Constitución Política de los Estados Unidos Mexicanos de 1917 y las Constituciones posteriores a la segunda guerra mundial, entre otras muchas.
>
> Desde este punto de vista, se puede considerar que los derechos fundamentales tienen una explicación y una necesidad histórica.
>
> De algún modo se puede considerar que los derechos fundamentales constituyen la línea más elevada del desarrollo jurídico del hombre.
>
> Por otro lado, también se puede razonar que los derechos humanos se nutren de los propios fenómenos sociales y que son, por decirlo de algún modo, la síntesis de los procesos sociales.
>
> Esto es claro si se considera que, en gran medida, los derechos sociales previstos en los artículos 27 y 123 de la Constitución Política de los Estados Unidos Mexicanos constituyen el producto de la interacción del proceso social que desembocó en la revolución mexicana de principios del siglo pasado.
>
> Es necesario recordar lo anterior, porque los derechos fundamentales no deben considerarse como el fruto contingente de una voluntad caprichosa de los actores políticos en turno, sino teoremas jurídicos éticos, históricos y sociales de las condiciones mínimas del ser humano en el contexto social.[259]

---

[258] Es importante señalar que la Constitución de los Estados Unidos de América, se promulgó el 17 de septiembre de 1787, en cambio la fundación de los Estados Unidos de América fue el 4 de julio de 1776 fecha en que el Segundo Congreso Continental representando a las 13 colonias firmó la Declaración de Independencia, por lo tanto es conveniente aclarar fechas incongruentes en lo dicho por García Torres.

[259] Gaceta del Senado, No. 166, Año. 2006, México D.F., martes 18 de abril, Senado de la República, ***Dictamen de las Comisiones unidas de Puntos Constitucionales y Estudios Legislativos, al que contiene el proyecto de decreto por el cual se adicionan dos párrafos al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos***, http://www.senado.gob.mx/sen60/sgsp/gaceta/?sesion=2006/04/18/1&documento=36

Es de esta forma como se plantea la siguiente adición:

> **Toda persona tiene derecho a la protección de sus datos personales**, así como al derecho de acceder a los mismos y, en su caso, obtener su rectificación, cancelación o destrucción en los términos que fijen las leyes.
>
> **La ley puede establecer supuestos de excepción a los principios que rigen el tratamiento de datos**, por razones de seguridad nacional, de orden público, seguridad, salud o para proteger los derechos de tercero

El día 18 de abril el dictamen fue aprobado por 77 votos, 5 abstenciones, turnándose a la Cámara de Diputados. Esta discusión, que se había mantenido congelada por más de dos años en el Congreso de la Unión, logró destrabarse, a pesar de las resistencias de sectores como el Consejo Coordinador Empresarial (CCE), entre otros, de acuerdo con diferentes posiciones que los legisladores habían manifestado.

De concretarse esta reforma constitucional, la cual todavía tiene que ser aprobada por la Cámara de Diputados y luego el comunicado de votación de congresos locales[260] a favor por al menos 16 de ellos, podría dar paso a la aprobación de la Ley de Datos Personales, iniciativas que estudiaremos más adelante.

En entrevista para El Universal,[261] Lina Ornelas, directora de Datos Personales del Instituto Federal de Acceso a la Información (IFAI), explicó que con esta reforma constitucional se da pie a la creación de una ley de datos personales, ya que hasta la fecha en México no existe regulación alguna de los datos que manejan las empresas privadas y el resto del gobierno federal.

C) Iniciativa de adición de un párrafo al artículo 6º de la Constitución presentada por la Diputada Cristina Portillo Ayala el 31 de mayo de 2006.

Aun ya aprobada por el Senado la anterior iniciativa de adición, se presento una más por parte de la diputada Cristina Portillo Ayala, dicho proyecto fue turnado a las Comisiones de Puntos Constitucionales de la Cámara de Diputados y se encuentra en proceso de dictamen. Cabe señalar que de la exposición de motivos no se encuentra ningún sustento que nos de luz de su implementación como un derecho fundamental, en cambio si nos da la pauta en cuanto a los principios fundamentales que rigen este derecho, mencionando los que la OCDE ha considerado. En mi parecer resulta un tanto extraño que ya aprobada una adición a un precepto constitucional que contiene el derecho fundamental de la protección de datos, se promueva una nueva iniciativa que contiene similar

---

[260] Documento por medio del cual las legislaturas estatales emiten un voto de aprobación o desaprobación de una reforma constitucional que le fue turnada con anterioridad por el Congreso de la Unión. QUINTANA VALTIERRA, Jesús y CARREÑO GARCÍA, Franco, ***Derecho Parlamentario y Técnica Legislativa en México***, Editorial Porrúa, México, 2006, pág. 430.

[261] SAÚL, Lilia, ***Destraban la ley de datos personales,*** El Universal, Sección: México, viernes 21 de abril de 2006. pág. 2.

disposición pero ubicada en otro artículo del máximo ordenamiento. La propuesta señala lo que sigue:

> Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. El respeto de estas normas estará sujeto al control de una autoridad independiente.[262]

Parece que la aportación importante es una referencia a lo que sería el *habeas data*, ya que previene un derecho para acceder a los datos recogidos y a obtener su rectificación. Por otro lado hace referencia a una autoridad independiente, lo que nos genera dudas, ya que en ningún momento se dice que exista otra autoridad para que una sea independiente, o en su caso alguna mención a la creación de un organismo especializado. A mi modo de ver esta propuesta esta fuera de tiempo y mal ubicada dentro de la Constitución.

D) Iniciativa que contiene proyecto de Decreto que reforma el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, presentada por el Senador José Alberto Castañeda Pérez el 9 de agosto de 2006.

Esta iniciativa, presentada a finales de la LIX legislatura, contempla la inclusión en el artículo 6º de la Ley fundamental, la protección a la intimidad, la vida privada, el honor y la propia imagen. Contempla la exposición de motivos:

> En México los derechos a la intimidad, honor y a la propia imagen sólo se encuentran parcialmente tutelados como consecuencia de la protección de otras garantías tales como la inviolabilidad de las comunicaciones privadas y la limitación a la libertad de imprenta. En materia penal, se castiga como delitos la revelación de secretos, la intromisión ilícita en sistemas y equipos de cómputo que cuenten con mecanismos de seguridad, y algunos delitos contra el honor como la difamación y la calumnia. En el ramo civil, se establece el daño moral, entre otras causas, por violaciones a la vida privada.
>
> El problema fundamental lo encontramos cuando la intimidad o privacidad del ser humano, su honor o su imagen se ven vulnerados por otros particulares y concretamente por la falta de clarificación en los límites del ejercicio de la libertad de expresión.
>
> Lo anterior ocurre porque los preceptos constitucionales antes señalados, no establecen **cuándo** la *libertad de expresión* afecta los derechos de terceros o **cuándo** la *libertad de imprenta* puede llegar a vulnerar la vida privada. De ahí la necesidad de contar con una legislación reglamentaria específica y apropiada que establezca de manera clara y con un criterio objetivo lo que comprende la vida privada o ámbito íntimo del individuo para así poder establecer con precisión los límites de estos dos derechos que en ocasiones parecen confrontarse estableciéndose una lucha entre la libertad de expresión y el derecho a la intimidad.

---

[262] ***Gaceta Parlamentaria, año IX, número 2021***, Cámara de Diputados, México, D.F., lunes 5 de junio de 2006, http://gaceta.diputados.gob.mx/

> El propósito principal de esta iniciativa de Ley, es el de incluir los derechos a la intimidad, honor y a la propia imagen para que sean reconocidos como derechos fundamentales.
>
> No podemos imaginar una vida digna y plena, si estamos ante la inseguridad de que, de manera sistemática, pudiéramos ser víctimas de intromisiones indebidas en nuestra esfera personalísima.
>
> Por consecuencia, en tanto derecho fundamental, los derechos a la intimidad, honor y a la propia imagen deben tener las características de todo derecho de esta categoría: máximo rango, máxima fuerza jurídica y máxima importancia del objeto y máximo grado de indeterminación. Es decir, debe ubicársele en la cúspide de los derechos tutelados por el ordenamiento, debe contar con mecanismos normativos que le impriman eficacia auténtica, debe otorgarse la máxima importancia al bien jurídico que tutela y emitir disposiciones genéricas que permitan su regulación en las normas secundarias y en la interpretación jurisprudencial.[263]

Notamos que habla textualmente de los requisitos que todo derecho fundamental debe de tener según Alexi, como ya lo citamos anteriormente (máximo rango, máxima fuerza jurídica y máxima importancia del objeto y máximo grado de indeterminación). Con esta reforma se da más certeza respecto de la protección a la vida privada, pero no se hace mención expresa de los datos personales y su regulación. Más bien esta reforma le traería paz a los personajes de una sociedad para evitar la intromisión en su vida privada y lo que se dice de ellos, claro que la protección es amplia, es contra actos de autoridad y de particulares. Establece la propuesta de adición al artículo 6º constitucional:

> Todas las personas físicas **tienen derecho al honor, a la intimidad personal y a la propia imagen.** El Estado debe respetarlos y hacerlos respetar, contra actos de las autoridades y de los particulares

Esta iniciativa se turnó a las Comisiones Unidas de Puntos Constitucionales y de Estudios Legislativos de la Cámara de Senadores.

E) Dictamen de las Comisiones Unidas de Puntos Constitucionales; y de Estudios Legislativos, segunda, el que contiene proyecto de Decreto que adiciona un segundo párrafo al artículo 6 de la Constitución Política de los Estados Unidos Mexicanos de 24 de abril de 2007.[264]

La Cámara de Diputados reformuló y sintetizó la llamada "Iniciativa de Chihuahua", originalmente elaborada por los gobernadores de los Estados de Aguascalientes, Chihuahua, Veracruz, Zacatecas y el Jefe de Gobierno del Distrito Federal. En sesión celebrada por la Cámara de Diputados del Congreso

---

[263] Gaceta del Senado, No. 14, Año. 2006, México D.F., miércoles 9 de agosto, Senado de la República, ***Iniciativa del Senador José Alberto Castañeda Pérez del grupo parlamentario del Partido Acción Nacional que contiene proyecto de Decreto que reforma el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos,*** http://www.senado.gob.mx/sgsp/gaceta/index2.php?sesion=2006/08/09/1&documento=23

[264] Gaceta del Senado, No. 101, Año. 2007, México D.F., martes 24 de abril, Senado de la República, **Dictamen de las Comisiones Unidas de Puntos Constitucionales; y de Estudios Legislativos, segunda, el que contiene proyecto de decreto que adiciona un segundo párrafo al artículo 6º de la Constitución Política de los Estados Unidos Mexicanos,** http://www.senado.gob.mx/sgsp/gaceta/?sesion=2007/04/24/1&documento=62

de la Unión, el 6 de marzo de 2007, se aprobó el Dictamen de las Comisiones Unidas de Puntos Constitucionales y de la Función Pública con Proyecto de Decreto que reforma el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos. Posteriormente el 8 de marzo del mismo año, la Mesa Directiva de la Cámara de Senadores del Congreso de la Unión recibió de su Colegisladora la minuta de referencia, turnándola a las Comisiones Unidas de Puntos Constitucionales y de Estudios Legislativos, Segunda, para su estudio y elaboración del dictamen correspondiente.

La Minuta con Proyecto de Decreto por el que se adiciona un segundo párrafo con VII fracciones al artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, tiene como principal función establecer los principios fundamentales que dan contenido básico al derecho de acceso a la información mismos que deberán regir a la Federación, los Estados y el Distrito Federal. Esta reforma permitirá garantizar que toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal sea pública y sólo pueda ser reservada temporalmente de manera excepcional por razones de interés público en los términos que fijen las leyes, toda vez que existen circunstancias en que la divulgación de la información pueda afectar un interés público valioso para la comunidad. Por ello, obliga a una ponderación conforme a la cual si la divulgación de cierta información puede poner en riesgo de manera indubitable e inmediata un interés público jurídicamente protegido, la información puede reservarse excepcionalmente de manera temporal. Asimismo, se señala que en la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Establece una limitación universal, sin temporalidad e infranqueable al derecho de acceso a la información pública: la que se refiere a la protección de la vida privada y de los datos personales. Esta información no puede estar sujeta al principio de publicidad, pues pondría en grave riesgo otro derecho fundamental: el derecho a la vida privada. Se propone que los datos que conciernen a la vida privada de los individuos y que obran en poder del Estado deben reservarse en tanto no exista un interés público acreditado que justifique plenamente su difusión, tema que la reforma introduce por primera vez en nuestra Carta Magna.

De esta manera en el Dictamen publicado en la Gaceta del Senado en su punto número 2 denominado "Objetivos esenciales" señala en función de los datos personales:

> Dicho de forma resumida, el decreto que propone la Colegisladora tiene los siguientes objetivos esenciales:
>
> ...
>
> 7.- Establecer que la única gran excepción a la publicidad la constituye el respeto a la vida privada de las personas. Los datos que se refieren a la intimidad de los mexicanos, es la única causal fundamental, permanente y no sujeta a plazo, de reserva de la información que posee el Estado.
>
> 8.- Propiciar la expedición de una legislación en materia de protección de datos personales que precise los límites entre la información pública y la

> información que se refiera a las personas físicas, identificadas o identificables, relativa a sus características físicas, morales, emocionales, a su vida afectiva y familiar, creencias o convicciones, estado de salud, preferencias sexuales u otras análogas que atañan a su intimidad.

En materia de acceso a la información el motivo de esta reforma radica en dar una homogeneidad a todas las legislaciones estatales, siendo indispensable una reestructuración a escala nacional de la implementación de este derecho, ya que al ser un derecho fundamental no debe tener modalidades distintas en función de situaciones propias de cada entidad federativa, como lo dice el dictamen, se busca un "hilo conductor" en un mismo sentido para que sin importar el nivel de gobierno toda persona tenga exactamente la misma certeza jurídica para ejercer su libertad de conocer los asuntos públicos del país.

Previene textualmente la adición del segundo párrafo con VII fracciones del artículo 6º de nuestra Constitución:

> Artículo 6o.- ...
>
> Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
>
> I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.
>
> **II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.**
>
> III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.
>
> IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.
>
> V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.
>
> VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.
>
> VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.

El dictamen fue aprobado por 111 votos y fue turnado a las legislaturas estatales para su trámite constitucional. En su discusión intervinieron los

Senadores: Alejandro Zapata Perogordo, Pedro Joaquín Coldwell, Pablo Gómez Álvarez, Ramón Muñoz Gutiérrez, Jorge Legorreta Ordorica y Dante Delgado.

Ahora bien, la aprobación de este dictamen y la eventual reforma a nuestra Carta Magna con esta adición, a mi modo de ver no le da el carácter de derecho fundamental a la protección de datos personales, es decir, esta adición lo que pretende es proteger los datos personales de los ciudadanos que obren en bases de datos, expedientes, procedimientos administrativos, etcétera, siempre y cuando los mismos sean de entidades públicas a los tres niveles de gobierno, creo también que esta adición viene a dar sustento a la ya existente regulación sobre datos personales que existe en la Ley Federal de Acceso a la Información Pública y Gubernamental. Es de reconocerse que esta reforma es un gran avance para la democracia en el país, para el derecho fundamental del acceso a al información pública y también garantiza la vida privada de las personas frente a los entes del Estado. Pero el vacío continúa, los entes privados pueden utilizar aún nuestros datos personales sin que exista ningún medio de defensa al alcance de los particulares.

3.- Protección a la vida privada en la Constitución Política de los Estados Unidos Mexicanos

Como hemos manifestado al inicio de este apartado, existen menciones constitucionales sobre la protección a la vida privada que configuran una incipiente protección, más no un derecho fundamental expreso sobre protección de datos personales, o más general, protección a la vida privada en Internet, así las cosas encontramos en varias disposiciones visos de dicha protección, como lo son los artículos 6º, 7º, 16, y el 133.

En este orden de ideas, la mayoría de los autores es consistente en afirmar que la protección a la vida privada tiene sus fundamentos en el artículo 16 de nuestra Constitución. En primer lugar Alejandro Reyes Krafft[265] señala: "El artículo 16 prohíbe las simples 'molestias' en la propiedad, es molestia porque atenta contra el derecho básico a la privacía que el Derecho reconoce, así como la inviolabilidad de las comunicaciones privadas y la libre circulación de la correspondencia." Por su parte el Maestro Ernesto Villanueva[266] nos dice: "En México el derecho a la privacidad está regulado por el artículo 7º constitucional, que prescribe como límite a la libertad de prensa el respeto a la vida privada. También es aplicable el artículo 16 de la Constitución primer párrafo... Esta garantía de seguridad jurídica es, sin duda, amplia y suficiente para garantizar el derecho a la privacidad de los individuos, pues regula con precisión los requisitos que debe reunir el mandamiento escrito mediante el que pueda afectarse o molestarse a la persona." Es de notarse que se habla de "privacidad" como un sinónimo de vida privada, esta cuestión de conceptos fue tratada a detalle en

[265] REYES KRAFFT, Alejandro, ***Protección de Datos Personales en México. Génesis Legislativa***, Revista de Derecho Informático, No. 100, Noviembre 2006, http://www.alfa-redi.org/rdi-articulo.shtml?x=7846
[266] VILLANUEVA, Ernesto, ***Derecho de la Información***, H. Cámara de Diputados-Miguel Angél Porrúa Editor, México, 2006, pág. 303.

nuestro primer capítulo, vemos que existe aun una confusión entre uno y otro término que se ha usado de forma indistinta junto con el de intimidad.

Por otra parte Rocío Ovilla Bueno, nos dice que el objeto del derecho a la intimidad es la protección de los datos e información personal proplas al ser humano. Este derecho va a evitar toda intromisión en la esfera privada del individuo. "El derecho a la intimidad está relacionado con la libertad de expresión, pues si bien todo ser humano tiene el derecho de expresarse libremente, esta libertad tiene como límite la esfera privada de un tercero"[267] de esta forma cita al artículo 6º de la ley fundamental como sustento, también indica que el artículo 7º hace referencia a la libertad de imprenta y al límite de la misma, que seguirá siendo el respeto a la vida privada de terceros, es de notarse que es la única parte de toda la Constitución donde se habla expresamente de "vida privada" que hemos adoptado como el concepto más valido por esta razón entre otras y sus limites que están señalados en la Ley de Imprenta la cual estudiaremos a detalle más adelante. Por último Ovilla Bueno establece que el artículo 16 constitucional también hace referencia al derecho a la intimidad, regulando la inviolabilidad de las comunicaciones. "Como podemos observar existen al menos tres fundamentos constitucionales de la protección de datos personales. A partir de aquí, hay varias leyes en México que contienen de forma dispersa una protección de datos".[268]

El autor mercantilista Pedro Alberto de Miguel Asensio, señala: "La protección a la privacidad se vincula con el artículo 16 de los Estados Unidos Mexicanos, que dispone que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones. Salvo con respecto a los datos personales en poder de los organismos públicos a los que se aplica la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental de 2002, en la legislación mexicana no existe todavía un sistema elaborado de protección de los datos personales, si bien sí existen disposiciones sectoriales."[269] En efecto De Miguel Asensio concuerda en señalar como fundamento constitucional de la protección de la vida privada el artículo 16, pero además nos aclara que únicamente existe la protección sobre datos personales en la LFTAIP, es importante destacar que a pesar de no existir un derecho fundamental expreso en la Constitución, la materia ya esta reglamentada en dicha ley, si bien no aplica a todos los sectores, sí existe una Dirección General de Protección de Datos Personales.

Para el experto en derecho a la información, Antonio Aveleyra, el fundamento existe también en el artículo 16 de la Ley Fundamental: "Podemos apreciar como la Constitución mexicana requiere declarar la protección a los datos personales o privados, aunque sí contempla las garantías relacionadas de inviolabilidad del domicilio (artículo 16 párrafo tercero), o de inviolabilidad de la correspondencia (artículo 16 párrafos segundo y cuarto). El avance de las TI y de los medios masivos y su penetración en la sociedad urge a los legisladores para proveer

---

[267] OVILLA BUENO, Rocío, ***La protección de los datos personales en México***, Editorial Porrúa, Brevlarios Jurídicos, No. 28, México, 2005, pág. 27.
[268] Ibidem, pág. 28.
[269] DE MIGUEL ASENSIO, Pedro Alberto, ***Derecho del Comercio Electrónico***, Editorial Porrúa, México, 2005, pág. 170-171.

leyes actualizadas para la protección de los derechos de las personas en la esfera de su confidencialidad y privacidad."[270]

El maestro Burgoa sostiene en su Diccionario de Derecho Constitucional, Garantías y Amparo, bajo la voz de "vida privada": Establece el artículo 7º constitucional, mediante su interpretación a *contrario sensu*, que la libertad de imprenta se podrá coartar o impedir cuando su ejercicio implique un ataque o falta de respeto a la vida privada". Y nos aclara: "El criterio que sirve de base para consignar esta restricción, nos parece demasiado vago, impreciso y lato, opinión que también abrigaron los Constituyentes de 1857".[271] Esta discusión ha existido de siempre, hasta que la jurisprudencia no se ocupe de ella, o en su momento una reforma integral a la Constitución y su respectiva ley reglamentaria nos den luz sobre el tema, pero el prestigiado constitucionalista, señala también como un fundamento constitucional de la vida privada el artículo 7º de la Carta Magna.

La obra de Gómez Robledo y Ornelas Núñez,[272] también señala los fundamentos que hemos sostenido: "En este sentido la Constitución Política de los Estados Unidos Mexicanos plasma el derecho a la vida privada como límite a la intromisión del Estado en el ámbito de la persona..., Por su parte, los artículos 6º y 7º constitucionales establecen como límite a la manifestación de las ideas y a la libertad de imprenta respectivamente, el ataque a los derechos de un tercero y *el respeto a la vida privada*. La libertad de expresar o publicar pensamientos encuentra entonces una restricción cuando con ello se menoscabe a la persona. Asumiendo que los datos personales se encuentran dentro de la esfera de la vida privada de una persona y que ésta debe ser protegida, surge el *deber del Estado de brindar protección a los datos personales de los ciudadanos*. Ahora bien el concepto de privacidad ha evolucionado a nivel internacional a partir del uso de las tecnologías de la información las cuales permiten que la información concerniente a las personas físicas sea tratada, es decir, recabada, utilizada, almacenada y transmitida para diversos fines tanto en el sector público como en el privado, comportando en ocasiones amenazas a la privacidad, derivadas de las injerencias arbitrarias o ilegales en dicha esfera de las personas."

Ya señaladas las posturas de la doctrina en cuanto el respeto a la vida privada en la Constitución federal, es oportuno hacer nuestras propias consideraciones analizando cada precepto y ampliándolo aún al artículo 133 constitucional.

En primer lugar el artículo 6º de la Constitución contempla la libertad de expresión y a la letra dice:

> Artículo 6o.- La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, **sino en el caso de** que ataque a la moral,

---

[270] AVELEYRA, Antonio, ***La comunicación de mensajes de datos personales en México. El predecible estado de arte: la administración pública los desarrollos privados y los esfuerzos legislativos 2003-2004***, Derecho Comparado de la Información, No. 4, Julio – Diciembre 2004, Instituto de Investigaciones Jurídicas, UNAM, pág. 3.

[271] BURGOA ORIHUELA, Ignacio, ***Diccionario de Derecho Constitucional, Garantías y Amparo***, Editorial Porrúa, México, 2005, pág. 437.

[272] GÓMEZ ROBLEDO, Alonso, ORNELAS NÚÑEZ, ***Protección de Datos Personales en México: El caso del Poder Ejecutivo Federal***, Instituto de Investigaciones Jurídicas, UNAM, México, 2007, pág. 14.

> los **derechos de tercero**, provoque algún delito o perturbe el orden público; el derecho a la información será garantizado por el estado.

Este numeral es importante ya que limita la esfera privada de los terceros, además que es el sustento del acceso a la información pública y gubernamental, que como ya mencionamos en su ley sectorial contempla un apartado de datos personales. Algo que aun no queda claro en relación a este principio constitucional es que en caso de que exista un conflicto entre el principio de publicidad y la necesidad de guardar reserva respecto de la información pública, se deberá resolver el mismo, mediante la evaluación del daño que pudiera causar la difusión de la información, o bien acreditando causas de interés público. También está pendiente en este precepto lo que tiene que ver con el entendido de que no existen derechos ilimitados, dado que estos hayan su acotamiento, en la protección de intereses superiores, que para el caso en concreto se refiere a la protección de la intimidad de las personas, por lo que la información que se refiera a la vida privada y los datos personales, deberá considerarse como confidencial, y será de acceso restringido en los términos que fijen las futuras leyes que legislen la materia de protección de datos. Ahora bien al consagrar como derecho fundamental el de la protección de datos no debe de ser ubicado en este numeral, es desafortunado, ya que esta libertad de expresión y acceso a la información están debidamente integradas y agregar la protección de datos como lo proponen la iniciativa estudiada supone hablar de las limitantes a este derecho fundamental sin darle su grado de independencia.

En este orden de ideas para apuntalar lo que el numeral protege, nos apegamos a lo que el prestigiado maestro Enrique Sánchez Bringas[273] nos dice en función de este derecho fundamental de libertad: "... se refiere a la libertad de expresión verbal que no debe ser objeto de impedimento judicial o administrativo sino en aquellos casos en que se ataque a la moral, los derechos de tercero, se provoque un delito o se perturbe el orden público."

En segundo lugar encontramos el artículo 7º de la Constitución federal, que consagra, el derecho fundamental de la libertad de imprenta:

> Artículo 7o.- es inviolable la libertad de escribir y publicar escritos sobre cualquiera materia. Ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, que **no tiene más límites que el respeto a la vida privada**, a la moral y a la paz publica. En ningún caso podrá secuestrarse la imprenta como instrumento del delito.

El respeto a la vida privada como límite a la libertad de imprenta es lo que consagra este numeral, como dijera Burgoa, se hace una interpretación a *contrario sensu*, para obtener mayor luz sobre la protección a la vida privada. Este concepto esta muy ligado a lo dispuesto por la polémica Ley de Imprenta que será tratada en su momento. Entonces como límite a la libertad de expresión encontramos el derecho a la vida privada, que debe ser respetado

---

[273] SÁNCHEZ BRINGAS, Enrique, ***Derecho Constitucional***, Editorial Porrúa, México, 2006, pág. 657.

para no conculcar el honor de las personas o exponerlas al desprecio ajeno. En este sentido resulta importante destacar que el Cuarto Tribunal Colegiado en Materia Civil del Primer Circuito ha señalado:

> Los artículos 6o. y 7o. de la Constitución Federal establecen el marco jurídico que a la vez que consagra el derecho a la libre manifestación de las ideas y la libertad de imprenta, les impone límites consistentes en que la manifestación de las ideas no debe ejercerse en forma que ataque la moral, los derechos de tercero, provoque algún delito o perturbe el orden público; la libertad de imprenta **tiene por límite el respeto a la vida privada**, la moral y la paz pública. Por su parte, el artículo **1o. de la Ley de Imprenta prevé lo que se considera como ataques a la vida privada, y en su fracción I establece que lo es toda manifestación o expresión hecha por la imprenta o que de cualquier otra manera circule en la opinión pública donde se expone a una persona al odio, desprecio o ridículo y que pueda causarle demérito en su reputación e intereses.** Como se advierte, en el supuesto de la fracción I resulta irrelevante que la información o manifestación sea falsa o verdadera. Basta que se exponga a una persona al odio, desprecio o ridículo. El decoro está integrado por el honor, el respeto, la circunspección, la honestidad, el recato, la honra y la estimación. Se basa en el principio de que a toda persona, por el hecho de serlo, se le debe considerar honorable, merecedora de respeto. La conculcación de este bien se configura en sentido negativo, cuando el sujeto activo, sin fundamento, daña a una persona en su honor o en la estimación que los demás tienen de ella en el medio social en que se desenvuelve y que es donde directamente repercute en su agravio. El honor es un bien objetivo que hace que la persona sea merecedora de confianza. Si una persona sufre una afectación en la consideración que de ella tienen los demás, se debe entender como una lesión a la estima que los demás le profesan, o sea, al trato con urbanidad y respeto que merece. El límite entre la libertad de expresión y la conducta ilegal del agente sólo puede establecerse mediante la ponderación de los derechos en presencia, para determinar si la restricción que se impone al derecho de información y expresión está o no justificada por la limitación que sufriría el otro derecho a la intimidad. Dada su función institucional, cuando se produzca una colisión entre ambos derechos, el de la información goza de una posición preferente, y las restricciones a ese derecho deben interpretarse de tal modo que su contenido esencial no resulte desnaturalizado. Tal valor preferente no es, sin embargo, absoluto. Si se le reconoce como garantía de la opinión pública, sólo puede legitimar intromisiones en otros derechos fundamentales que guarden congruencia con esa finalidad, o sea, que resulten relevantes para la formación de la opinión pública. Carecerá de protección cuando se ejercite de manera desmesurada a ese fin.[274]

Al decir de Burgoa,[275] la Suprema Corte no se ha ocupado del problema, pues únicamente en una ejecutoria ha establecido la distinción entre la vida privada y la vida pública de un funcionario público para los efectos de la constitucionalidad de la crítica escrita que contra la actuación de éste se dirija. Nos dice la tesis:

> La Constitución establece, en su artículo séptimo, entre las limitaciones a la libertad de imprenta, **el respeto a la vida privada, debiendo entenderse por ésta, la que se refiere a las actividades del individuo como particular, en contraposición a la vida pública,** que comprende los actos del funcionario o empleado en el desempeño de su cargo; de modo que para determinar si un

[274] ***Semanario Judicial de la Federación y su Gaceta***, Novena Época, t. XVII, marzo de 2003, tesis I.4º.C.57 C, pág. 1709; CD-ROM IUS: 184669.
[275] Op. cit. pág.437-438.

> acto corresponde a la vida privada o a la pública, no hay que atender al lugar en que dicho acto se ejecutó, sino al carácter con que se verifica, pues de no ser así, fácilmente se evitaría el castigo, atribuyendo a una persona acciones desarrolladas en lugar público, aunque dañaran gravemente su reputación

Estos criterios de jurisprudencia, no nos dan luz sobre la protección a al vida privada en general y menos aún en la esfera tecnológica, por lo tanto existen de forma incipiente incluso para el mundo real, que podemos esperar para el mundo virtual.

En tercer lugar encontramos el numeral que viene a dar mayor protección a la vida privada dentro de la Constitución, este es el artículo 16, que se presta a mayor rango interpretativo sobre todo en el aspecto de la inviolabilidad de la correspondencia. El párrafo primero refiriéndose al no poder ser molestado en nuestra persona:

> Artículo 16. **Nadie puede ser molestado en su persona**, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

La libre circulación de las comunicaciones privadas y de correspondencia se protegen dentro del texto constitucional en el artículo 16, párrafos noveno, décimo y penúltimo.

> ...**Las comunicaciones privadas son inviolables**. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacia de las mismas. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del ministerio público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada...
>
> **Las intervenciones autorizadas se ajustaran a los requisitos y límites previstos en las leyes**. Los resultados de las intervenciones que no cumplan con estos, carecerán de todo valor probatorio.
>
> **La correspondencia que bajo cubierta circule por las estafetas, estará libre de todo registro**, y su violación será penada por la ley.

La protección constitucional a la privacidad se traduce en realidad a una protección a la persona misma y a su intimidad. La Constitución garantiza, con ello, incluso el carácter secreto de las comunicaciones privadas, sea cual sea su contenido. El párrafo noveno señala que las comunicaciones privadas son inviolables, esto es, hace una referencia general, sin distingos de ninguna índole, a la naturaleza de las comunicaciones y de la forma en que éstas se presentan; no se restringe la disposición constitucional sólo a los escritos impresos, sino que el concepto alcanza a cualquier grabación que en medios electrónicos, ópticos o digitales se realice, incluyendo, dice Carbonell, las que se generen mediante el uso de tecnologías como Internet[276]

---

[276] Carbonell, Miguel, ***Los Derechos Fundamentales en México***, México, Universidad Nacional Autónoma de México, 2004, pp. 139-140.

La garantía de inviolabilidad de las comunicaciones protege, a su vez, otros derechos fundamentales, como la libertad de expresión, la intimidad y la autonomía de la persona. Respecto a la valoración que la Corte ha realizado sobre la validez de las pruebas consistentes en comunicaciones privadas, este máximo Tribunal ha llevado su interpretación no sólo a la protección de la correspondencia frente a la autoridad pública, sino hasta cuestionar la ilicitud en la obtención de la información por parte de particulares, negando la validez de las pruebas en cuya obtención se ha vulnerado la privacidad del titular (véanse las tesis aisladas: "COMUNICACIONES PRIVADAS. LAS PRUEBAS OFRECIDAS DENTRO DE UN JUICIO CIVIL, OBTENIDAS POR UN GOBERNADO SIN RESPETAR LA INVIOLABILIDAD DE AQUÉLLAS, CONSTITUYEN UN ILÍCITO CONSTITUCIONAL, POR LO QUE RESULTAN CONTRARIAS A DERECHO Y NO DEBEN ADMITIRSE POR EL JUZGADOR CORRESPONDIENTE"[277] Y "COMUNICACIONES PRIVADAS. EL DERECHO A SU INVIOLABILIDAD, CONSAGRADO EN EL ARTÍCULO 16, PÁRRAFO NOVENO, DE LA CONSTITUCIÓN FEDERAL, ES OPONIBLE TANTO A LAS AUTORIDADES COMO A LOS GOBERNADOS, QUIENES AL TRANSGREDIR ESTA PRERROGATIVA INCURREN EN LA COMISIÓN DE UN ILÍCITO CONSTITUCIONAL[278]").

Particular interés revisten los anteriores criterios en los cuales la Corte destaca la relevancia del derecho a la privacidad, no exigiendo sólo la conducta pasiva de la autoridad, sino incluso vedando a cualquier persona la posibilidad de hacer uso de estos elementos para su beneficio, en detrimento del afectado. Se trata pues de una garantía absoluta, que involucra a autoridades y gobernados en sus relaciones, incluso privadas, lo cual hace destacar el alcance de la protección constitucional y la relevancia que implica la protección a las comunicaciones en este rubro.

La protección a la correspondencia y papeles ha sido elevada a la categoría de derecho fundamental dado que los datos y papeles se hacen extensivos a la persona en sí, al extremo de que su violación se traduce en una afectación al ser mismo, a su dignidad y a su esfera de privacidad.[279] El penúltimo párrafo del artículo 16 constitucional establece:

> "La correspondencia que bajo cubierta circule por las estafetas estará libre de todo registro, y su violación será penada por la ley."

Al respecto Carbonell nos recuerda[280] lo que la Corte ha definido y entiende por correspondencia, al establecer el órgano de control constitucional, en una tesis aislada, lo siguiente:

> **VIOLACIÓN DE CORRESPONDENCIA, CONCEPTO DE CORRESPONDENCIA EN EL DELITO DE** Para la configuración del delito de violación de correspondencia es irrelevante que haya sido un sobre que contenía un giro telegráfico el que abrió indebidamente el inculpado, al no estar dirigido a él, toda vez que debe considerarse como correspondencia una comunicación escrita, entendiéndose por tal, una carta o comunicación con el sobrescrito cerrado o con la plica cerrada y

---

[277] Tesis aislada, ***Semanario Judicial de la Federación y su Gaceta, t. XII***, diciembre de 2000, Novena Época, segunda sala, tesis 2 CLX/2000, p. 428.
[278] Tesis aislada, ***Semanario Judicial de la Federación y su Gaceta, t. XII***, diciembre de 2000, Novena Época, segunda sala, tesis 2 CLX/2000, p. 428.
[279] Castro V., Juventino, ***Garantías y Amparo***, México, décimo primera edición, Editorial Porrúa, 2000.
[280] Carbonell, Miguel, ***op. cit.*** p. 142.

> sellada, un pliego igualmente guardado en el sobrescrito o la plica, un despacho telegráfico o telefónico con igual protección y cualquier otra comunicación escrita análoga[281].

Como puede apreciarse, la Corte ha sostenido que el término correspondencia se hace extensivo a toda comunicación escrita contenida en una comunicación con el sobrescrito cerrado, que puede ser también una llamada telefónica o cualquier otra comunicación de similar naturaleza.

Con base en la definición de la Corte, que data de 1991, cabe preguntarse si se puede incluir, dentro de esas "comunicaciones análogas", a la transmisión de datos o comunicados enviados a través de correo electrónico o contenidos en medios ópticos. En mi opinión, la respuesta es contundentemente afirmativa, toda vez que en 1991, año en que se produjo el criterio de la Corte, la intensidad en el tráfico de datos aún no se presentaba, pero es indudable que en la actualidad la cantidad de datos y comunicaciones rebasa el uso de los medios considerados entonces como ortodoxos, consistentes en el correo, telégrafo, fax, etcétera. Por otra parte lo que busca proteger el derecho, no es la conservación de los empaques, sobre o protecciones de las cartas o comunicaciones, lo que se busca es la salvaguarda de un bien mayor consistente en el respeto a la capacidad de expresar y escribir los pensamientos, la inviolabilidad de la persona en cuanto a su intimidad, por lo que el constituyente no buscó proteger sólo la libre circulación de correspondencia, sino el derecho a la intimidad del individuo, reconocido éste como un valor de la mayor trascendencia en su dignidad.

Desde luego que la Corte no hizo referencia expresa a los medios electrónicos, pero al establecer la posibilidad de analogar los medios de comunicación, no cabe duda que la protección constitucional se hace necesariamente extensiva por igual a los mensajes contenidos en correo electrónico, o insertos en cualquier otro medio óptico. Mayor relevancia adquiere la protección constitucional, cuando reconocemos que en realidad la información, datos o comunicados que mayor importancia económica representan, generalmente constan en medios electrónicos, lo cual ha provocado la proliferación de violaciones a los sistemas que los contienen, por encima de las agresiones que puedan darse a sobres y paquetes cerrados.

Por último nos referimos al artículo 133 de la Carta Magna. Ya en nuestro anterior capítulo hicimos referencia a la jurisprudencia de la Suprema Corte de Justicia de la Nación que nos dice que los Tratados Internacionales tienen una jerarquía inmediatamente inferior a la Constitución, pero superior a las leyes federales; lo anterior es plenamente aplicable a los derechos fundamentales.

México ha suscrito y ratificado las siguientes Convenciones Internacionales relacionadas con los derechos fundamentales de protección a la vida privada: Declaración Universal de Derechos Humanos (1948) artículo 12; los artículos 5,

---

[281] Tesis aislada, ***Semanario Judicial de la Federación y su Gaceta, t. VIII***, Junio de 1991, Octava Época, tribunales colegiados de circuito, p. *459*.

9 y 18 de la Declaración Americana de Derechos y Deberes del Hombre (1948); el Pacto Internacional de Derechos Civiles y Políticos (1966) artículo 17; la Convención Americana de Derechos Humanos o Pacto de San José de Costa Rica (1969) artículo 11); la Convención sobre los Derechos del Niño (1989) artículo 16; Asimismo la Convención Internacional de Telecomunicaciones (Nairobi 1982) artículos 18, 22 y 27, publicada en el Diario Oficial de la Federación en Junio 29 de 1984, actualmente sustituída por la Constitución y Convenio Internacional de Telecomunicaciones, de Niza, Francia, 30 de Junio de 1989, ratificada por México el 26 de Abril de 1991, y publicada en el DOF el 3 de Marzo de 1992. Por lo tanto la protección existe y es Ley en nuestro país.

II.- La protección a la vida privada en la legislación federal.[282]

La vida privada ha sido legislada de forma sectorial, es decir vamos a encontrar de forma aislada y en diferentes materias de nuestro ordenamiento jurídico dicha protección, es importante destacar que no existe a la fecha una ley que regule en específico la protección de los datos personales, pero existen varias iniciativas que están pendientes de ser estudiadas por el Poder Legislativo y serán materia de nuestro estudio. Este apartado va a estar sistematizado no por jerarquías sino por orden alfabético, como aparece citada nuestra legislación en la página de Internet de la Cámara de Diputados, que contiene todas las disposiciones jurídicas federales entre otras el Código Civil Federal, el Código de Comercio, la Ley sobre el Delito de Imprenta, Ley Federal de Protección al Consumidor, Ley Federal de Derechos de Autor o la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, solo por mencionar algunas.

1.- Código Civil Federal.

Existe la figura del daño moral dentro de nuestro ordenamiento civil federal. Salvador Ochoa[283] siguiendo a Ernesto Villanueva nos dice que el daño moral: "... es aquel que se infringe contra el honor, la imagen y la dignidad de la persona. El artículo 1916 del Código Civil define el daño moral como 'la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspectos físicos, o bien en la consideración que de sí misma tienen los demás'."

En reforma publicada en el Diario Oficial de la Federación el viernes 13 de abril de 2007, derogaron diversas disposiciones del Código Penal Federal, referentes a los delitos de injurias, difamación y calumnia, (del artículo 350 al 363 del Código Penal Federal) por considerar que deben ser los jueces de lo civil quienes resuelvan si las personas, periodistas y comunicadores actúan dentro o fuera de la ley al difundir su información u opiniones, eliminando la pena de

---

[282] Para la elaboración de este apartado fue fundamental la obra del maestro Antonio. M. Aveleyra, ***"La transición democrática en México, el derecho a la libertad informática, y el derecho a la intimidad"*** que contiene un cuadro denominado ***"El derecho a la privacidad en la legislación federal secundaria de México"*** disponible online en: http://profesor.sis.ula.mx/aveleyra/comunica/privacidad/tdm.htm

[283] OCHOA OLVERA, Salvador, ***La demanda por Daño Moral***, Montealto Editores, México, 1999, pág. 42. Se recomienda esta obra si se quiere abundar en el tema.

prisión a quien abuse de la libertad de expresión, dejando abierta la posibilidad de demandar la reparación del daño causado a terceros en la vía civil. Para este fin se reforma el Código Civil Federal, con el ánimo de hacer las adecuaciones pertinentes a los artículos 1916 y 1916 Bis, donde se contempla lo referente a la reparación del daño moral por quien en ejercicio del derecho de opinión, crítica, expresión o información, contravenga lo dispuesto en los artículos 6º y 7º Constitucionales, de esta forma se puede regular los casos en los que existan excesos en el ejercicio de la libertad de expresión, previniendo además de la reparación del daño moral correspondiente, la obligación de la rectificación o respuesta de la información difundida en el mismo medio donde fue publicada, con el mismo espacio y la misma circulación y audiencia.

Como se puede advertir, existe en la reforma, la tutela de dos principios jurídicos relevantes, como son el derecho a la libre expresión, por un lado, y el derecho a la vida privada, al honor y a la buena reputación por otro. Con esta reforma se puede decir que se da un gran avance en materia de tutela a la libertad de expresión pero a la vez se protege la vida privada.

El texto del artículo después de la reforma es como sigue:

> **Artículo 1916.-** Por daño moral se entiende **la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, o bien en la consideración que de sí misma tienen los demás.** Se presumirá que hubo daño moral cuando se vulnere o menoscabe ilegítimamente la libertad o la integridad física o psíquica de las personas.
>
> Cuando un hecho u omisión ilícitos produzcan un daño moral, el responsable del mismo tendrá la obligación de repararlo mediante una indemnización en dinero, con independencia de que se haya causado daño material, tanto en responsabilidad contractual como extracontractual. Igual obligación de reparar el daño moral tendrá quien incurra en responsabilidad objetiva conforme a los artículo 1913, así como el Estado y sus servidores públicos, conforme a los artículos 1927 y 1928, todos ellos del presente Código.
>
> La acción de reparación no es transmisible a terceros por acto entre vivos y sólo pasa a los herederos de la víctima cuando ésta haya intentado la acción en vida.
>
> El monto de la indemnización lo determinará el juez tomando en cuenta los derechos lesionados, el grado de responsabilidad, la situación económica del responsable, y la de la víctima, así como las demás circunstancias del caso.
>
> Cuando el daño moral haya afectado a la víctima en su decoro, honor, reputación o consideración, el juez ordenará, a petición de ésta y con cargo al responsable, la publicación de un extracto de la sentencia que refleje adecuadamente la naturaleza y alcance de la misma, a través de los medios informativos que considere convenientes. En los casos en que el daño derive de un acto que haya tenido difusión en los medios informativos, el juez ordenará que los mismos den publicidad al extracto de la sentencia, con la misma relevancia que hubiere tenido la difusión original.
>
> **Estarán sujetos a la reparación del daño moral de acuerdo a lo establecido por este ordenamiento y, por lo tanto, las conductas descritas se considerarán como hechos ilícitos:**

> I. El que comunique a una o más personas la imputación que se hace a otra persona física o moral, de un hecho cierto o falso, determinado o indeterminado, que pueda causarle deshonra, descrédito, perjuicio, o exponerlo al desprecio de alguien;
>
> II. El que impute a otro un hecho determinado y calificado como delito por la ley, si este hecho es falso, o es inocente la persona a quien se imputa;
>
> III. El que presente denuncias o querellas calumniosas, entendiéndose por tales aquellas en que su autor imputa un delito a persona determinada, sabiendo que ésta es inocente o que aquél no se ha cometido, y
>
> **IV. Al que ofenda el honor, ataque la vida privada o la imagen propia de una persona.**
>
> La reparación del daño moral con relación al párrafo e incisos anteriores deberá contener la obligación de la rectificación o respuesta de la información difundida en el mismo medio donde fue publicada y con el mismo espacio y la misma circulación o audiencia a que fue dirigida la información original, esto sin menoscabo de lo establecido en el párrafo quinto del presente artículo.
>
> La reproducción fiel de información no da lugar al daño moral, aun en los casos en que la información reproducida no sea correcta y pueda dañar el honor de alguna persona, pues no constituye una responsabilidad para el que difunde dicha información, siempre y cuando se cite la fuente de donde se obtuvo.[284]

Nos establece dicho artículo que cuando un hecho u omisión ilícitos produzcan el daño moral,[285] el responsable tendrá que repararlo mediante una indemnización. Si bien es cierto esta norma no tutela directamente el derecho a la vida privada, sí puede ser utilizada para obtener por la vía indicada una indemnización en caso de violación al multicitado derecho. En general la protección del Código Civil Federal es deficiente en materia de protección a la vida privada. Por otra parte el artículo 1916 bis, que también tuvo una adición con la reforma del 13 de abril de 2007, tiene una importante mención sobre dos artículos primordiales de la Constitución que ya hemos estudiado:

> **Artículo 1916 Bis.-** No estará obligado a la reparación del daño moral quien ejerza sus derechos de opinión, crítica, expresión e información, en los términos y con las limitaciones de los artículos 6o. y 7o. de la Constitución General de la República

---

[284] ***Código Civil Federal***, Cámara de Diputados, Reforma publicada en el Diario Oficial el viernes 13 de abril de 2007, http://www.diputados.gob.mx/LeyesBiblio/doc/2.doc

[285] Como un buen ejemplo tenemos el caso entre la periodista argentina Olga Wornat vs. Marta Sahagún de Fox, donde también se vio envuelto el semanario Proceso, el martes 23 de enero de 2007 la Primera Sala de los Civil del Tribunal Superior de Justicia del Distrito Federal absolvió a la revista mencionada, luego de que, en una primera instancia, un juez civil lo había declarado causante de daño moral. Entre los argumentos validados por los magistrados destaca el hecho de que la libertad de expresión y de imprenta predominan jurídicamente cuando se trata de asuntos de interés público y de hechos veraces. Y, como parte de las pruebas finalmente valoradas, está el consentimiento que había dado Sahagún para que se divulgaran pasajes de su vida privada. Otro importante argumento fue que la información fue de interés público porque en el momento de presentar la demanda Sahagún era la esposa del Presidente de la República y realizaba actividades públicas. Indicaron: "Las personalidades públicas, que ejercen funciones públicas o resultan implicadas en asuntos de relevancia pública, deben soportar un cierto mayor riesgo de injerencia en sus derechos de personalidad que las personas privadas". Aunque el Tribunal Superior de Justicia no lo dice explícitamente al hacer su valoración comparativa entre libertad de expresión y daño moral a una persona, sería importante puntualizar que éste debe prevalecer sólo en los casos en que el mismo sea mayor al beneficio que produzca la difusión de la información. CARRASCO ARAIZAGA, Jorge, ***Sahagún contra la pared***, Semanario Proceso, No. 1578, México, 28 de enero de 2007, pp. 6-13

> En todo caso, quien demande la reparación del daño moral por responsabilidad contractual o extracontractual deberá acreditar plenamente la ilicitud de la conducta del demandado y el daño que directamente le hubiere causado tal conducta.
>
> En ningún caso se considerarán ofensas al honor las opiniones desfavorables de la crítica literaria, artística, histórica, científica o profesional. Tampoco se considerarán ofensivas las opiniones desfavorables realizadas en cumplimiento de un deber o ejerciendo un derecho cuando el modo de proceder o la falta de reserva no tenga un propósito ofensivo.

El que ejerza los derechos de libre expresión y acceso a la información no está obligado a reparar daño moral, más las limitaciones que establecen dichos numerales, recordemos en el caso del 7º, la vida privada. Si trasladamos esta protección al uso de Internet nos encontramos en una enorme orfandad, en palabras de Salvador Ochoa nos queda muy claro: "El derecho al honor de las personas a través de Internet a la fecha, carece de una tutela judicial integral, ya que el mismo es, y puede ser generado en sistemas jurídicos diferentes en donde se produce la conducta o se realiza el hecho y la clandestinidad del mismo provocan su impunidad, por lo tanto la materialidad de la acción aparece en la recepción de la comunicación, pero al no existir sujeto responsable no existe proceso ni sanción."[286]

Al decir de Rocío Ovilla Bueno,[287] el artículo 1834 bis, del Código Civil Federal incluye una protección a datos personales:

> **Artículo 1834 Bis.**- Los supuestos previstos por el artículo anterior se tendrán por cumplidos **mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología**, siempre que la información generada o comunicada en forma íntegra, **a través de** dichos medios sea atribuible a las personas obligadas y accesible para su ulterior consulta.
>
> En los casos en que la ley establezca como requisito **que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán generar, enviar, recibir, archivar o comunicar la información que contenga los términos exactos en que las partes han decidido obligarse, mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuye dicha información a las partes y conservar bajo su resguardo una versión íntegra de la misma para su ulterior consulta**, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

El numeral se refiere en específico a la forma de los contratos, y la protección a la que se refiere Ovilla Bueno es en aquellos casos en que se tenga que corroborar ante fedatario público lo que ya se había enviado mediante medios electrónicos. A mi entender, lo que se procura es que no exista falsedad en lo que se ha transmitido y lo que consta ante el fedatario público, es un principio

---

[286] OCHOA OLVERA, Salvador, ***Protección civil del honor***, Editorial Porrúa, México, 2006, pág. 81.
[287] OVILLA BUENO, Rocío, ***La protección de los datos personales en México***, Editorial Porrúa, Breviarios Jurídicos, No. 28, México, 2005, pág. 29 y 30.

de veracidad pero no un principio protector, por lo tanto no creo que podamos adjudicar una tutela a los datos personales en el Código Civil Federal.

2.- Código de Comercio.

Los autores Reyes Krafft y Aveleyra coinciden en señalar que en este ordenamiento existe protección a la vida privada, principalmente en lo que se refiere a la institución del secreto que tiene el comerciante para llevar de su propia manera la contabilidad y la comunicación que se refiere a la presentación para su examen de la totalidad de la contabilidad del comerciante. Transcribimos los artículos respectivos:

> **Artículo 42.- No se puede hacer pesquisa de oficio por tribunal ni autoridad alguna, para inquirir si los comerciantes llevan o no el sistema de contabilidad** a que se refiere este capítulo.
>
> **Artículo 43.- Tampoco podrá decretarse, a instancia de parte, la comunicación, entrega o reconocimiento general de los libros, registros, comprobantes, cartas, cuentas y documentos de los comerciantes**, sino en los casos de sucesión universal, liquidación de compañía dirección o gestión comercial por cuenta de otro o de quiebra.
>
> **Artículo 44.**- Fuera de los casos prefijados en el artículo anterior, **sólo podrá decretarse la exhibición de los libros, registros y documentos de los comerciantes, a instancia de parte o de oficio, cuando la persona a quien pertenezcan tenga interés o responsabilidad en el asunto en que proceda la exhibición.**[288]

El artículo 42 prescribe el derecho la reserva que se tiene para llevar su propio sistema de contabilidad. Luego la disposición 43 autoriza la comunicación únicamente en los casos en que se verse sobre un juicio denominado "universal", por su parte el numeral 44, nos dice que la exhibición de los libros procede a instancia de parte o de oficio cuando la persona a quien pertenezca la contabilidad tenga interés o responsabilidad en el asunto.

3.- Código Federal de Instituciones y Procedimientos Electorales.

Este ordenamiento constituye uno de los pilares de las reformas político-electorales que se han gestado en nuestro país a partir de 1977, supone también la constitución de un padrón electoral confiable (reclamo de los actores políticos de oposición). Esta adopción de un padrón electoral confiable al decir de Gómez Robledo supuso: "...un punto de tensión entre el derecho a la protección a la privacidad en su vertiente de protección a los datos personales y la protección de los derechos políticos de los ciudadanos".[289]

Para crear dicho padrón los ciudadanos tuvimos que entregar información sensible muy relevante, como nuestro nombre, lugar y fecha de nacimiento, edad, sexo, domicilio, firma, huella digital y nuestra fotografía. Para que dicho

---

[288] ***Código de Comercio***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/3.doc

[289] GÓMEZ ROBLEDO, Alonso, ORNELAS NÚÑEZ, ***Protección de Datos Personales en México: El caso del Poder Ejecutivo Federal***, Instituto de Investigaciones Jurídicas, UNAM, México, 2007, pág. 24.

padrón fuera confiable, tanto partidos políticos como ciudadanos participaron en el proceso de depuración, divulgándose así los datos personales de todos nosotros, pero esta difusión que se da en todo el proceso electoral (listas nominales, entrega del padrón electoral a disposición de partidos para su consulta y revisión, exhibición de listas nominales en las secciones electorales para que los votantes corroboren su inclusión en el padrón, etcétera) no es indiscriminada, ya que existen normas en la materia, para proteger dicha información:

> **Artículo 135**
>
> 3. **Los documentos, datos e informes que los ciudadanos proporcionen al Registro Federal de Electores, en cumplimiento de las obligaciones que les impone la Constitución y este Código, serán estrictamente confidenciales** y no podrán comunicarse o darse a conocer, salvo cuando se trate de juicios, recursos o procedimientos en que el Instituto Federal Electoral fuese parte, para cumplir con las obligaciones previstas por este Código en materia electoral y por la Ley General de Población en lo referente al Registro Nacional Ciudadano o por mandato del juez competente.[290]

La edición comentada del COFIPE por el Instituto Federal Electoral,[291] nos dice en función de este apartado: "En lo referente a la confidencialidad de los datos del RFE, se trata efectivamente de una limitación al derecho a la información. Esta restricción impide a las autoridades electorales, dar a conocer los datos de los ciudadanos, a menos que se trate de juicios." Para apoyar este supuesto encontramos una tesis de la Tercera Época la Sala Central del Tribunal Electoral del Poder Judicial de la Federación: VOTO. SU CONFIDENCIALIDAD Y SECRETO SE TRANSGREDEN SI SE REVELAN DATOS PROPORCIONADOS POR LOS CIUDADANOS, FUERA DE LAS HIPOTESIS LEGALES PERMITIDAS

En segundo lugar podemos decir que las listas nominales exhibidas en las secciones electorales son extracto del padrón y solo incluyen el nombre de los electores, sin abundar en los datos ya proporcionados en la integración del padrón, así nos dice el siguiente numeral:

> **Artículo 155**
> 1. Las **listas nominales** de electores son las relaciones elaboradas por la Dirección Ejecutiva del Registro Federal de Electores que **contienen el nombre de las personas incluidas en el Padrón Electoral**, agrupadas por distrito y sección, a quienes se ha expedido y entregado su Credencial para Votar.

Por su parte el artículo 156 señala que los Partidos Políticos no pueden darle un uso distinto al padrón electoral que no sea el consagrado en la ley, que puede ser el de revisión, formulación de observaciones de la información que contiene tanto las listas nominales como el padrón electoral:

> **Artículo 156**

---

[290] ***Código Federal de Instituciones y Procedimientos Electorales***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/5.doc

[291] ***Código Federal de Instituciones y Procedimientos Electorales. Comentado***, Instituto Federal Electoral, México, 2003, pág. 258.

> 4. Las listas nominales de electores que se entreguen a los partidos políticos **serán para su uso exclusivo y no podrán destinarse a finalidad u objeto distinto al de revisión del Padrón Electoral**. Cuando un partido político no desee conservarlas, deberá reintegrarlas al Instituto Federal Electoral.

Con la reforma de 30 de junio de 2005, que crea el Libro Sexto, del voto de los mexicanos residentes en el extranjero, también se crean listas nominales para los electores en el extranjero, de esta forma se garantiza su confidencialidad:

> **Artículo 280**
>
> 3. En todo caso, **el personal del Instituto y los partidos políticos están obligados a salvaguardar la confidencialidad de los datos personales contenidos en las listas nominales de electores residentes en el extranjero**. La Junta General Ejecutiva dictará los acuerdos e instrumentará las medidas necesarias para tal efecto.

Si bien esta protección existe, la misma fue insuficiente, como ya lo hemos dicho en otro espacio de esta obra la adquisición por parte de *Choice Point* del padrón electoral, nos hace pensar que faltan medidas de seguridad adecuadas para salvaguardar los datos personales de los electores mexicanos.

En cuanto a corrección y rectificación de datos no existe una disposición expresa, pero una tesis relevante de la Sala Superior del Tribunal Electoral[292] nos da luz al respecto:

> LISTA NOMINAL DE ELECTORES. ES DE LA EXCLUSIVA COMPETENCIA DE LOS CIUDADANOS TRAMITAR LOS CAMBIOS DE DATOS PERSONALES EN LA
> Del contenido del artículo 150 del Código Federal de Instituciones y Procedimientos Electorales, se desprende que es obligación de los ciudadanos dar aviso de su cambio de domicilio ante la oficina del Instituto Federal Electoral más cercana a éste. Asimismo, el artículo 151, párrafo 1, inciso c) del referido Código establece el derecho de los ciudadanos para solicitar la rectificación ante la oficina del Instituto Federal Electoral, cuando consideren haber sido indebidamente incluidos o excluidos de la lista nominal de la sección correspondiente a su domicilio. **Por lo anterior de una interpretación sistemática y funcional de dichos preceptos, se debe llegar a la conclusión de que el Registro Federal de Electores no puede realizar modificación alguna de los datos personales de los ciudadanos**, por cambio de domicilio, sin la participación de ellos a través de la correspondiente solicitud.

Si bien es cierto la tesis anterior habla de que el RFE no puede realizar modificación alguna de los datos de los ciudadanos, una interpretación a *contrario sensu* determinaría que los ciudadanos pueden hacer dicho trámite.

4.- Código Federal de Procedimientos Civiles.

[292] Recurso de apelación SC-I-RAP-500/94, interpuesto por el Partido de la Revolución Democrática, con fecha de resolución 22 de junio de 1994.

Siguiendo a Alejandro Reyes Krafft, en este ordenamiento encontramos una disposición relacionada con la vida privada:

> **ARTICULO 90.-** Los terceros están obligados, en todo tiempo, a prestar auxilio a los tribunales, en las averiguaciones de la verdad. Deben, sin demora, exhibir documentos y cosas que tengan en su poder, cuando para ello fueren requeridos.[293]

"Al igual que en materia procesal, las legislaciones que hablan de los periodos de recabar información para las autoridades, incluyen una gran pluralidad de normas fincando a cargo de todos la obligación de proporcionar los datos que ayuden a las autoridades interesadas para instruir sus criterios."[294] Podemos decir que es obligación de los ciudadanos obsequiar a las autoridades datos personales que sirvan en la obtención de la verdad, aquí vemos de nueva cuenta que el interés público está por encima de lo privado, es otro de esos puntos de contacto entre ambas esferas.

5.- Código Federal de Procedimientos Penales.

El artículo 192 de este cuerpo legal, nos habla de la reserva de declarar a cualquier persona que tenga un vínculo afectivo o de respeto, en clara muestra de protección a la vida privada del acusado y para evitar que las indagatorias se vean entorpecidas.

> ARTÍCULO 192.- **No se obligará a declarar al tutor, curador, pupilo o cónyuge del acusado, ni a sus parientes por consanguinidad o afinidad en la línea recta ascendente o descendente, sin limitación de grados, y en la colateral hasta el tercero inclusive, ni a los que estén ligados con el acusado por amor, respeto o gratitud.** Si estas personas tuvieren voluntad de declarar, se les recibirá su declaración y se hará constar esta circunstancia.[295]

Este supuesto resguarda en primer lugar la vida privada del acusado y a la vez el interés público se ve salvaguardado ya que la declaración de estas personas puede ser falsa u orientada a favorecer al acusado.

6.- Código Fiscal de la Federación.

En este ordenamiento federal encontramos lo que se le ha denominado secreto fiscal, que esta legislado en el artículo 69. Alonso Gómez – Robledo[296] al hablar del secreto en general nos dice: "De esta suerte al referirnos al secreto en general, debemos considerarlo como la obligación que corre a cargo de una persona, organización o autoridad de guardar en reserva, fuera de la vista de

---

[293] *Código Federal de Procedimientos Civiles*, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/6.doc

[294] REYES KRAFFT, Alfredo Alejandro, ***Protección de datos personales en México. Génesis legislativa***, Revista de Derecho Informático, No. 100, noviembre de 2006. http://www.alfa-redi.org/rdi-articulo.shtml?x=7846

[295] ***Código Federal de Procedimientos Penales***, Cámara de Diputados, Reformas del 10 de abril de 2007, http://www.diputados.gob.mx/LeyesBiblio/doc/7.doc,

[296] ***Voto particular del Comisionado Alonso Gómez-Robledo al Recurso de Revisión No. 1825/05 del Comisionado Alonso Lujambio Irazábal***, Instituto Federal de Acceso a la Información Pública y Gubernamental, México, 2005, http://ifai.gob.mx/resoluciones/2005/votos/1852_1.pdf

terceros, información personal y patrimonial que alguien le ha proporcionado, ya sea por la actividad mercantil de los primeros, o por disposición legal. En principio en todo "secreto" habrá tres partes involucradas: la parte que proporciona información, la parte que recibe y debe custodiar la información, y el tercero del que se oculta dicha información". El artículo 69 del Código Fiscal dice lo siguiente:

> ARTÍCULO 69.- **El personal oficial que intervenga en los diversos trámites relativos a la aplicación de las disposiciones tributarias estará obligado a guardar absoluta reserva en lo concerniente a las declaraciones y datos suministrados por los contribuyentes** o por terceros con ellos relacionados, así como los obtenidos en el ejercicio de las facultades de comprobación.
>
> Dicha reserva no comprenderá los casos que señalen las leyes fiscales y aquéllos en que deban suministrarse datos a los funcionarios encargados de la administración y de la defensa de los intereses fiscales federales, a las autoridades judiciales en procesos del orden penal o a los Tribunales competentes que conozcan de pensiones alimenticias, o en el supuesto previsto en el artículo 63 de este Código.
>
> Dicha reserva tampoco comprenderá la información relativa a los créditos fiscales exigibles de los contribuyentes, que las autoridades fiscales proporcionen a las sociedades de información crediticia que obtengan autorización de la Secretaría de Hacienda y Crédito Público de conformidad con la Ley de Agrupaciones Financieras.
>
> La reserva a que se refiere el párrafo anterior no será aplicable tratándose de las investigaciones sobre conductas previstas en el artículo 400-Bis del Código Penal Federal, que realice la Secretaría de Hacienda y Crédito Público.
>
> Cuando las autoridades fiscales ejerzan las facultades a que se refiere el artículo 215 de la Ley del Impuesto sobre la Renta, la información relativa a la identidad de los terceros independientes en operaciones comparables y la información de los comparables utilizados para motivar la resolución, sólo podrá ser revelada a los tribunales ante los que, en su caso, se impugne el acto de autoridad, sin perjuicio de lo establecido en los artículos 46, fracción IV y 48, fracción VII de este Código.
>
> Solo por acuerdo expreso del Secretario de Hacienda y Crédito Público se podrán publicar los siguientes datos por grupos de contribuyentes: nombre, domicilio, actividad, ingreso total, utilidad fiscal o valor de sus actos o actividades y contribuciones acreditables o pagadas. Mediante acuerdo de intercambio recíproco de información, suscrito por el Secretario de Hacienda y Crédito Público, se podrá suministrar la información a las autoridades fiscales de países extranjeros, siempre que se pacte que la misma sólo se utilizará para efectos fiscales y se guardará el secreto fiscal correspondiente por el país de que se trate.

De esta forma se obliga a los servidores públicos a guardar reserva respecto de la información proporcionada por los contribuyentes o por terceros con ellos relacionados, así como los datos obtenidos por ese personal en el ejercicio de sus facultades de comprobación, tratándose de medios electrónicos los datos

que se obtengan del contribuyente para su certificado digital no formarán parte del secreto fiscal.

El citado artículo 69 del Código Fiscal de la Federación, establece como excepciones a la absoluta reserva a la que obliga en materia de documentación e información fiscal, a las siguientes:

- Los casos que señalen las leyes fiscales.
- Aquellos en que deba suministrarse información a los funcionarios encargados de la administración *y* de defensa de los intereses del fisco federal.
- La que deba proporcionarse a las autoridades judiciales en procesos del orden penal.
- La que deba proporcionarse a los tribunales competentes que conozcan de pensiones alimenticias.
- En el supuesto del artículo 63 del Código citado (para motivar las resoluciones de la Secretaría de Hacienda y Crédito Público y cualquier otra autoridad u organismo descentralizado competente en materia de contribuciones federales).
- En materia de créditos fiscales exigibles que las autoridades fiscales proporcionen a las Sociedades de Información Crediticia debidamente autorizadas para funcionar como tales.

En el caso de que un servidor público llegase a divulgar cualquier información que señala el artículo 69 se le impondrá un sanción penal de 1 a 6 años de prisión (artículo 114-B del mismo ordenamiento).

Por último es importante destacar la postura del IFAI en relación al secreto fiscal en el tercer considerando del recurso de revisión 243/06[297]:

> **Tercero.** En su escrito de alegatos, el Servicio de Administración Tributaria reiteró que la información solicitada está clasificada como reservada en virtud de que se actualiza el secreto fiscal, en términos de lo previsto en el artículo 14, fracción II de la Ley, en relación con el artículo 69 del Código Fiscal de la Federación.
> El artículo 14, fracción II de la Ley establece que se considera como información reservada la relativa a los secretos comercial, industrial, fiscal, bancario, fiduciario u otro considerado como tal por una disposición legal.

Es entonces información reservada el secreto fiscal.

7.- Código Penal Federal.

El ordenamiento penal mexicano es de los pocos cuerpos legales que ha tenido adaptaciones a partir de las nuevas tecnologías y en específico del uso de Internet. El Capítulo I del Título Tercero del Código Penal Federal, denominado "Delitos en Materia de Vías de Comunicación y Violación de la Correspondencia" contiene varios tipos penales que protegen la vida privada de los mexicanos.

---

[297] ***Resolución del Recurso de Revision 234/06, resuelto por la Comisionada María Marvan Laborde,*** Instituto Federal de Acceso a la Información Pública Gubernamental, México, 22 de marzo de 2006. http://www.ifai.gob.mx/resoluciones/2006/243.pdf

Con reforma publicada en el Diario Oficial de la Federación el lunes 17 de mayo de 1999, se modifica el artículo 167 primer párrafo y su fracción VI entre otras disposiciones. Este numera a la letra dice:

> ARTÍCULO 167.-Se impondrán de uno a cinco años de prisión y de cien a diez mil días multa:
>
> VI.- **Al que dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales**, por medio de las cuales se transfieran señales de audio, de video o de datos;[298]

Vemos entonces que ahora nuestro Código Penal Federal hace referencia a comunicaciones alámbricas o inalámbricas, de fibra óptica, telefónicas, satelitales o telegráficas, donde se transmitan señales de audio video o datos, es decir cualquier tipo de comunicación que sea interrumpida o interferida por vía telefónica, conexión a Internet, alámbrica o inalámbrica, conexión vía televisión satelital o datos transmitidos por fibra óptica, constituyen un delito, este es un gran avance, vale la pena pensar que toda la información que transmitimos por Internet utiliza este tipo de tecnologías.

Por otra parte en cuanto a la violación de correspondencia encontramos el artículo 173, *supra* podemos encontrar a mayor detalle comentarios y jurisprudencia que igualan a las comunicaciones escritas con las electrónicas extendiéndose así la protección a Internet. Es actualmente conocido que la correspondencia no se da únicamente a través de los medios convencionales, es decir vía el servicio postal y los de mensajería, pues con los adelantos tecnológicos, ésta puede ser a través de los *messengers*[299], vía fax o por mensajes escritos de telefonía celular, por lo tanto es notorio que la inviolabilidad de correspondencia como se entendía anteriormente no corresponde a la realidad actual. Nos dice el citado artículo:

> **Artículo 173.**- Se aplicarán de tres a ciento ochenta jornadas de trabajo en favor de la comunidad:
> **I.- Al que abra indebidamente una comunicación escrita que no esté dirigida a él, y**
> **II.- Al que indebidamente intercepte una comunicación escrita que no esté dirigida a él, aunque la conserve cerrada** y no se imponga de su contenido.
> Los delitos previstos en este artículo se perseguirán por querella.

---

[298] ***Código Penal Federal***, Cámara de Diputados, Reforma publicada en el Diario Oficial el viernes 13 de abril de 2007, http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf

[299] **Mensajería instantánea**.- Los mensajeros instantáneos o *messengers* son un conjunto de programas que utilizan el protocolo TCP IP que sirven para enviar y recibir mensajes instantáneos con otros usuarios conectados a Internet u otras redes, además saber cuando están disponibles para hablar. Los mensajeros instantáneos más utilizados son ICQ, *Yahoo! Messenger, MSN Messenger, AIM (AOL Instant Messenger)* y *Google Talk* (que usa el protocolo abierto *Jabber*). Estos servicios han heredado algunas ideas del viejo, aunque aún popular, sistema de conversación IRC. Cada uno de estos mensajeros permite enviar y recibir mensajes de otros usuarios usando los mismos software clientes, sin embargo, últimamente han aparecido algunos clientes de mensajerías que ofrecen la posibilidad de conectarse a varias redes al mismo tiempo (aunque necesitan registrar usuario distinto en cada una de ellas). También existen programas que ofrecen la posibilidad de conectarte a varias cuentas de usuario a la vez. ***Wikipedia. La enciclopedia libre***, http://es.wikipedia.org/wiki/Mensajer%C3%ADa_Instant%C3%A1nea

Sería oportuno que el artículo 173 previniera textualmente: "Al que abra indebidamente una comunicación escrita, o la accese a través de medios electrónicos, electromagnéticos, u ópticos, que no esté dirigida a él" tal y como lo dijera el "Proyecto de Iniciativa de Ley que Reforma y Adiciona Diversas Disposiciones del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal, con objeto de penalizar lo referente a delitos informáticos."[300] Dicho Proyecto contenía una interesante propuesta para poner como bien jurídico tutelado los datos personales, decía el artículo 399Ter, de dicha Iniciativa:

> **Artículo 399-ter.** Se aplicará la pena de prisión de dos a cinco años y de 100 a 300 días de multa al que:
> I. **Sin estar autorizado, se apodere, altere, utilice o modifique, en perjuicio de un tercero, datos reservados de carácter personal, familiar o de negocios que se hallen registrados en ficheros, programas, códigos, comandos, soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.**

Dicho proyecto fue turnado a las Comisiones de Justicia y Comunicaciones y Transportes de aquella legislatura, pero nunca fue dictaminado. Llama poderosamente la atención que se hablaba del anterior nombre del Código Penal Federal, cuando era aplicable incluso en el Distrito Federal, denotando desconocimiento de las facultades de la Cámara de Diputados para legislar en la materia.

El artículo 174 contiene la excepción referente a los padres que abren o interceptan las comunicaciones escritas dirigidas a sus hijos menores de edad y los tutores respecto de las personas que se hallen bajo su dependencia, así como también entre cónyuges.

Con la reforma de 1999,[301] también se crea un nuevo Capítulo dentro del Título noveno denominado "Revelación de secretos y acceso ilícito a sistemas y equipos de Informática", el nombre del Capítulo Segundo es: "Acceso ilícito a sistemas y equipos de computo".

La reforma incluyó, cinco nuevos tipos penales, relacionados íntimamente a la irrupción ilícita de sistemas y equipos de cómputo, únicamente haciendo caso omiso a las diversas conductas tipificables como son el fraude y el robo mediante el uso de Internet. Así en cuanto a lo que es la protección a la vida privada de las personas encontramos dentro de estos nuevos delitos el que sigue:

> **Artículo 211 bis 1**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática

---

[300] Gaceta Parlamentaria Año III, No. 474 miércoles 22 de marzo de 2000, ***Proyecto de Iniciativa de Ley que Reforma y Adiciona Diversas Disposiciones del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal, con objeto de penalizar lo referente a delitos informáticos***, http://gaceta.diputados.gob.mx/Gaceta/2000/mar/20000322.html

[301] Publicada en el ***Diario Oficial de la Federación***, segunda sección del lunes 17 de mayo de 1999.

> protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
> Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Los demás tipos penales de igual manera castigan la misma conducta pero los sujetos pasivos son el Estado o las Instituciones Financieras. El tipo penal descrito implica la intromisión no autorizada contenida en un sistema o equipo de informática, donde tendríamos que interpretar que entender por ello, ya que hoy en día también los teléfonos celulares de tercera generación son considerados equipos con sistemas integrados. Dicha intromisión implica una violación a nuestra esfera privada, ya que en nuestro equipo de cómputo podemos tener miles de datos sensibles, por lo tanto esta protección es adecuada pero no suficiente.

La reforma se da a raíz de las intromisiones de que fueron objeto diversos sitios *web* del gobierno federal, como la página de Internet de la Secretaría de Hacienda y Crédito Público, posteriormente la del Senado de la República y la de la Cámara de Diputados,[302] los legisladores mexicanos se abocaron desde, mediados de noviembre de 1998, a la tarea de articular el andamiaje legislativo-punitivo, que en el corto plazo permitiera la prevención y penalización de estas conductas.

El apartado regula y penaliza el acceso subrepticio a los sistemas y equipos de cómputo tanto públicos como privados; así como de la tutela y protección de la información oficial, comercial y personal, contenida en dichas computadoras.

Cabe destacar en un primer lugar que los representantes de la industria informática, académica y financiera nacional están ausentes así como la Comisión de Ciencia y Tecnología que no aparecen en los procesos de discusión y elaboración de la reforma.[303] Siendo ellos los principales agentes de estas tecnologías, hubieran dotado de un importante matiz tecnológico-jurídico y por supuesto de la imprescindible especialización, representatividad y legitimidad sectorial que en nuestros tiempos requiere la labor legislativa e incluso hubieran aportado una visión de protección a los datos personales que han sido materia de discusión desde hace ya varios años.

En segundo lugar es notable la desproporción e inequidad existente entre las penalidades y sanciones pecuniarias enumeradas por los numerales que incluyó la reforma, para sancionar íntima y selectivamente las diferentes modalidades o hipótesis materiales de lo que en estricto apego a la ley debería de ser un

---

[302] Existió una ciberprotesta a nivel mundial encabezada por un grupo de *hackers* en apoyo a Kevin Mitnick condenado a prisión por realizar actos de piratería electrónica, el ataque fue en contra de diferentes sitios de la www a nivel mundial. En México atacaron la Cámara de Diputados, ID Software y la Guía Virtual de México, violando la seguridad de acceso. Este se convierte en el tercer ataque a páginas del Gobierno Federal, incluyendo, los ataques en abril de 1998 a la página del Senado y de la Secretaría de Hacienda. **Hackers *hacen de las suyas en* site *de Cámara de Diputados,*** Reforma Sección Interfase, Lunes 22 de febrero de 1999, pág 7A.

[303] Según la información de Luis Antonio Hernández en ***"La reforma al Código Penal, apenas un avance"*** en su columna *"Internet y Legislación"*, Lunes 3 de mayo de 1999, *El Universal*, sección *Universo de la Computación*.

mismo delito. Se establecen criterios discriminatorios determinados según la calidad de las personas físicas y morales, o bien del Estado que hayan sido víctimas de los delincuentes informáticos. Esto demuestra el imperio del Estado mexicano aún sobre el resto de las organizaciones sociales y mercantiles que aún por su naturaleza guardan información comercial incuantificable, a mi modo de ver es un desden a la información que se posee de los ciudadanos por parte de personas físicas o morales en equipos de computo o bases de datos. De no ser así no se encuentra otra explicación a la disparidad existente entre las sanciones establecidas por la reforma al Código Penal Federal, ya que son de seis meses a dos años de prisión y de cien a trescientos días de salario mínimo vigente de multa, en aquellos casos en que se trate de personas físicas o morales del dominio privado, pero cuando se trataré de órganos estatales dígase legislativo, ejecutivo y judicial, en sus tres niveles, federal, local o municipal, la sanción es de uno a cuatro años de prisión y doscientos a seiscientos días multa.

Pareciera entonces que la información y datos personales de particulares no recibe igual importancia que la del Estado, debería existir congruencia en esa penalidad. La conducta que castiga es la más usual en el uso de las redes computacionales es decir el *hacking*[304] solamente, de lo cual deducimos la definición que nuestra legislación da al *hacker*[305] siendo "todo aquel que sin autorización modifique, destruya, provoque pérdida de información, conozca o copie información contenida en sistemas o equipos de informática ya sea de particulares, del Estado o instituciones que integran el sistema financiero", siendo este concepto algo de lo más rescatable de la reforma, olvidándose completamente de muchas otras conductas delictivas que tienen como instrumento el Internet, como los fraudes, el *cracking*[306], el *phreaking*[307], entre otras.

En resumen, podemos afirmar categóricamente que las expectativas generadas por la publicación de este ordenamiento, evidentemente, superaron su contenido y aplicación práctica, el cual involuntariamente representa apenas un

---

[304]Es sorprendente saber como existe toda una subcultura alrededor de esta actividad, así en 1984 del trabajo de Steven Levy, ***"Hackers: Heroes of the Computer Revolution"***, se examina la evolución de la Etica *Hacker*, un sexteto de credos que surgieron de las actividades de los *hackers* "pioneros" a finales de los cincuentas: "1.- Entrégate siempre al imperativo de Transmitir! El acceso a ordenadores y cualquier otra cosa que pueda enseñarte sobre como funciona el mundo debe ser limitado y total. 2.- Toda la información debe ser libre. 3.- Desconfía de la autoridad-Promueve la descentralización. 4.- Los *hackers* deben ser juzgado por su *hacking*, no por criterios falsos como títulos, edad, raza o posición. 5.- Puedes crear arte y belleza en un ordenador. 6.- Los ordenadores pueden cambiar tu vida a mejor" Este código ético forma la base política de las actividades de los *hackers* modernos. Dell Books, New York, 1984, pág 26.

[305]Con referencia a la definición de un *hacker*, podemos decir que las mismas varían de acuerdo con la posición socio-política del grupo o individuo que lo defina. Así podemos decir que dentro de la subcultura hacker se entiende al mismo como: "entusiastas de la informática que tienen un interés ardiente en aprender acerca de los sistemas informáticos y como usarlos de formas innovadoras" según Dorothy Denning, ***Concerning Hackers Who Break Into Computer Systems.*** en *Proceedings of the 13th National Computer Security Conference*, Octubre 1990. Esta definición, por tanto, no incluye a los *hackers* malignos que deliberadamente rompen sistemas y borran ficheros, sino a esos *hackers* que exploran sistemas simplemente por el reto intelectual y que no dejan indicios de sus actos.

[306]Al hablar de *cracks*, nos referimos a los programas o rutinas que permiten inutilizar los sistemas de protección establecidos por el titular de los derechos de propiedad intelectual sobre una aplicación informática. Dentro de los numerosos tipos de *cracks* existentes, destacan los que permiten seguir utilizando un programa de demostración una vez superado el periodo de prueba establecido.

[307]Es la técnica de fraude en materia de telefonía analógica y digital. Uno de los métodos más utilizados fue el de las denominadas "cajas de colores", que emitían distintas frecuencias, en función del resultado perseguido. Las utilizaban para efectuar llamadas sin cargo al transferir un número extraño a la "caja de colores".

avance en cuanto a la estructuración de la definición, tipificación y reglamentación no sólo de delitos informáticos sino de toda la gama de ordenamientos que requieren ser adecuados a las nuevas tecnologías de la información incluyendo claro está, la protección a la vida privada. Si bien es cierto que existe ya toda una protección en relación a la vida privada y su virtual ejercicio dentro de Internet o los medios electrónicos, es también cierto que existe todavía un gran vació sobre varios tópicos como son las conductas lesivas al bien jurídico del acceso a la información pública, la violación a y ataques a los datos personales en específico.

Por último es importante señalar que con la más reciente reforma del viernes 13 de abril del 2007, desaparecieron los delitos contra el honor, la moral, injuria y calumnia que estaban en los hoy derogados artículos 350 a 363, y que con la reforma pasan de ser delitos a ser objetos de indemnización por la vía civil como ya estudiamos.

8.- Ley de Información Estadística y Geográfica.

Este ordenamiento establece la confidencialidad de los datos proporcionados por los ciudadanos en la elaboración de estadísticas:

> ARTICULO 5o.- **La Ley garantiza a los informantes de datos estadísticos la confidencialidad de los que proporcionen**. El Ejecutivo expedirá las normas que regulen la circulación y aseguren el acceso del público a la información estadística y geográfica producida.

También destaca el derecho que tienen los informantes a corregir sus datos cuando consideren que los mismos son erróneos, un tipo de *habeas data* en materia estadística:[308]

> ARTICULO 37.- Los informantes, en su caso, **podrán exigir que sean rectificados los datos que les conciernan, al demostrar que son inexactos, incompletos, equívocos u obsoletos**, y denunciar ante las autoridades administrativas y judiciales todo hecho o circunstancia que demuestre que se ha desconocido el principio de confidencialidad de los datos o la reserva establecida por disposición expresa, en el ejercicio de las facultades que esta Ley confiere a las unidades que integran los sistemas nacionales.
>
> Para proteger los intereses del solicitante, cuando proceda, deberá entregársele un documento en donde se certifique el registro de la modificación o corrección. Las solicitudes correspondientes se presentarán ante la misma autoridad que captó la información registrada.

Nos dice Reyes Krafft:[309] "Esta ley garantiza a los informantes de datos estadísticos la confidencialidad de los datos que proporcionen, es particularmente importante aclarar que, de acuerdo con lo dispuesto por esta ley y su reglamento, los datos obtenidos para fines estadísticos no tienen validez legal".

---

[308] ***Ley de Información Estadística y Geográfica***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/41.doc

[309] REYES KRAFFT, Alejandro, Op. Cit. pág. 19.

9.- Ley de Instituciones de Crédito.

En esta ley se establece otro tipo de secreto, el denominado bancario, Luis Manuel Méjan[310] opina que es una "institución de naturaleza dual, es decir, que es una institución de derecho privado en tanto que regula operaciones entre comerciantes, operaciones típicamente mercantiles y regula las relaciones entre clientes y bancos; pero es una institución de derecho público por varias razones: se refiera a su ejercicio por el Estado, sea una actividad vigilada por un órgano desconcentrado, entre en la esfera competencial de algunas autoridades, suponga determinadas cargas procesales y pueda llegar a caer en la esfera de lo penal." En nuestra legislación, el secreto bancario es expresamente regulado en el artículo 117 de la Ley de Instituciones de Crédito, que a la letra dice:

> **Artículo 117.- La información y documentación relativa a las operaciones y servicios a que se refiere el artículo 46 de la presente Ley, tendrá carácter confidencial, por lo que las instituciones de crédito, en protección del derecho a la privacidad de sus clientes y usuarios que en este artículo se establece, en ningún caso podrán dar noticias o información de los depósitos, operaciones o servicios,** incluyendo los previstos en la fracción XV del citado artículo 46, **sino al depositante, deudor, titular, beneficiario, fideicomitente, fideicomisario, comitente o mandante, a sus representantes legales o a quienes tengan otorgado poder para disponer de la cuenta o para intervenir en la operación o servicio.**
>
> Como excepción a lo dispuesto por el párrafo anterior, las instituciones de crédito estarán obligadas a dar las noticias o información a que se refiere dicho párrafo, cuando lo solicite la autoridad judicial en virtud de providencia dictada en juicio en el que el titular o, en su caso, el fideicomitente, fideicomisario, fiduciario, comitente, comisionista, mandante o mandatario sea parte o acusado. Para los efectos del presente párrafo, la autoridad judicial podrá formular su solicitud directamente a la institución de crédito, o a través de la Comisión Nacional Bancaria y de Valores.[311]

Podemos entonces decir que el contenido del secreto bancario se ha entendido en sentido amplio, es decir, que deberá protegerse la información relativa a cualquier tarea o función de tipo bancaria, tanto de los movimientos financieros, como de los directamente involucrados. Por lo tanto, dentro del secreto bancario se protegerá la información relativa a:

1. Las operaciones financieras cualquiera que sea su naturaleza; 2. Datos confidenciales que en razón de la confianza y actividad profesional del banquero le han sido confiados por sus clientes; 3. A la vida privada del cliente.

Por su parte, Acosta Romero[312] afirma que "no forman parte del secreto bancario aquellas cuestiones que son meramente de información general que

---

[310] MÉJAN, Luis Manuel, ***El secreto bancario***, Biblioteca FELABAN, Bogotá Colombia, 1994, pág. 83.
[311] ***Ley de Instituciones de Crédito***, Cámara de Diputados, reforma de 30 de diciembre de 2005, http://www.diputados.gob.mx/LeyesBiblio/doc/43.doc
[312] ACOSTA ROMERO, Miguel, ***Nuevo derecho bancario***, Editorial Porrúa, México, 1995, pág. 331.

no comprenden datos específicos y que por otra parte también pudieran obtenerse por medios de publicidad".

Finalmente podemos afirmar que la información de naturaleza bancaria de los individuos cae bajo el rubro de información personal o datos personales, cuyo adecuado manejo, acceso, distribución y protección ha sido ya previsto por algunos países de Europa y Latinoamérica, estableciendo mecanismos claros de protección y defensa como Institutos de Protección de Datos o el *habeas data*, frente a las violaciones a las garantías individuales y derechos fundamentales de los individuos.

10.- Ley de Vías Generales de Comunicación.

Esta legislación contempla dentro de su articulado algunas disposiciones sobre la obligación que tienen los empleados y funcionarios en comunicaciones de guardar secreto en lo que respecta a los mensajes cuya transmisión este a su cargo. Veamos un ejemplo:

> ARTICULO 383.- Los empleados y funcionarios de comunicaciones eléctricas, dedicados al servicio, están obligados a guardar secreto absoluto y riguroso en lo que respecta al contenido de los mensajes cuya transmisión o recepción haya estado a su cargo, o de los que tengan conocimiento por razón de su empleo, y a no dar ningún informe con relación a los mismos, sino a los signatarios, destinatarios o a la autoridad competente.[313]

Existen penas severas e incluso la pena de prisión que va de 10 días a 3 meses, a quienes incumplan lo establecido por esta disposición.

11.- Ley Federal contra la Delincuencia Organizada

Por decreto publicado en el Diario Oficial de la Federación el 3 de julio de 1996, en vigor al día siguiente, el Constituyente Permanente, reformo y adiciono los artículos 16, 20 fracción I y penúltimo párrafo, 21, 22 y 73 fracción XXI de la Constitución Política de los Estados Unidos Mexicanos para permitir la intervención de comunicaciones privadas, siendo promulgada el 7 de diciembre de 1996. Dicha Ley surge según Raúl Plascencia Villanueva[314] como "reacción a las modernas y técnicas y métodos que usan los delincuentes organizados" Este cuerpo legal en sus artículos del 16 al 28 señala los supuestos y la manera en que la autoridad judicial podrá autorizar la intervención de las comunicaciones privadas, los artículos 26 y 27 introducen dos tipos penales referidos a los servidores públicos que intervengan comunicaciones privadas sin autorización judicial.

12.- Ley Federal de Protección al Consumidor

---

[313] ***Ley de Vías Generales de Comunicación***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/73.doc

[314] PLASENCIA VILLANUEVA, Raúl, ***Ley Federal contra la Delincuencia Organizada*** en ***Anuario Jurídico 1996***, UNAM, Instituto de Investigaciones Jurídicas, pág. 69.

En otras partes de nuestro trabajo hemos de tocar temas relacionados con este ordenamiento, que resulta de cabal importancia en nuestro estudio. La Ley Federal de Protección al Consumidor es promulgada el 22 de diciembre de 1992, en su artículo primero reconoce una serie de derechos básicos que con reforma publicada en el Diario Oficial de la Federación el 4 de febrero de 2004, dio cabida a dos principios muy importantes: en primer lugar la protección contra la publicidad engañosa y abusiva, donde podríamos encuadrar el *spam* y en segundo lugar la protección del consumidor en las transacciones en las que utiliza medios electrónicos o de cualquier otra tecnología y la adecuada utilización de sus datos, es decir resguarda los datos personales de los ciudadanos en las transacciones comerciales.

También esta reforma introduce en los artículos 16 a 18bis restricciones en relación al empleo de la información sobre los consumidores con fines mercadotécnicos lo que se convierte en un avance en la materia.

> **ARTÍCULO 16.-** Los proveedores y empresas que **utilicen información sobre consumidores con fines mercadotécnicos o publicitarios están obligados a informar gratuitamente a cualquier persona que lo solicite si mantienen información acerca de ella.** De existir dicha información, deberán ponerla a su disposición si ella misma o su representante lo solicita, e informar acerca de qué información han compartido con terceros y la identidad de esos terceros, así como las recomendaciones que hayan efectuado. La respuesta a cada solicitud deberá darse dentro de los treinta días siguientes a su presentación. **En caso de existir alguna ambigüedad o inexactitud en la información de un consumidor, éste se la deberá hacer notar al proveedor o a la empresa, quien deberá efectuar dentro de un plazo de treinta días contados a partir de la fecha en que se le haya hecho la solicitud, las correcciones que fundadamente indique el consumidor**, e informar las correcciones a los terceros a quienes les haya entregado dicha información.
>
> *Párrafo reformado DOF 04-02-2004*
>
> Para los efectos de esta ley, se entiende por fines mercadotécnicos o publicitarios el ofrecimiento y promoción de bienes, productos o servicios a consumidores.
>
> *Párrafo adicionado DOF 04-02-2004*[315]

Nos dice el experto en comercio electrónico Alberto de Miguel Asensio: "El artículo 16 LFPC reconoce el derecho de acceso, al imponer a las empresas que utilicen información sobre consumidores con fines de promoción de productos o servicios la obligación de informar gratuitamente, la información sobre él de la que disponen."[316] Así como esta opinión confluye la de Alejandro Reyes Krafft sobre este artículo en especial. Más adelante la ley dice:

> **ARTÍCULO 17.-** En la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor; de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la Procuraduría.
>
> *Párrafo reformado DOF 04-02-2004*

---

[315] ***Ley Federal de Protección al Consumidor***, Cámara de Diputados, Reformas publicadas el 4 de febrero de 2004, http://www.diputados.gob.mx/LeyesBiblio/doc/113.doc

[316] DE MIGUEL ASENSIO, Pedro Alberto, ***Derecho del Comercio Electrónico***, Editorial Porrúa, México, 2005, pág. 174.

> **El consumidor podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad.** Asimismo, el consumidor podrá exigir en todo momento a proveedores y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, **que la información relativa a él mismo no sea cedida o transmitida a terceros**, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial.
>
> *Párrafo adicionado DOF 04-02-2004*

Es en esta disposición donde encontramos la protección en contra del correo no deseado con fines comerciales o *spam*.[317] Este artículo contempla dos postulados primordiales, por una parte el derecho que tiene el consumidor de exigir al proveedor el no ser molestado con publicidad por cualquier medio incluido en estos su dirección electrónica. Y por otra parte incluye el derecho de exigir a los proveedores que la información que posean de los consumidores no sea transmitida a terceros, lo que por lo general implica la venta de bases de datos donde, dicha información se convierte en un bien con valor económico del cual no hemos dado nuestro consentimiento para su comercialización y además no obtenemos ningún beneficio con el lucro de la misma.

> **ARTÍCULO 18 BIS.- Queda prohibido a los proveedores y a las empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios y a sus clientes, utilizar la información relativa a los consumidores con fines diferentes a los mercadotécnicos o publicitarios**, así como enviar publicidad a los consumidores que expresamente les hubieren manifestado su voluntad de no recibirla o que estén inscritos en el registro a que se refiere el artículo anterior. Los proveedores que sean objeto de publicidad son corresponsables del manejo de la información de consumidores cuando dicha publicidad la envíen a través de terceros.
>
> *Artículo adicionado DOF 04-02-2004*

De nueva cuenta encontramos el derecho del consumidor de no recibir publicidad no deseada, siendo una prohibición expresa a los proveedores. También existe la prohibición de utilizar la información que posee el proveedor de los consumidores, con fines diferentes a los mercadotécnicos o publicitarios, como podría ser el uso para fines ilícitos como secuestros o para fines discriminatorios, por razón de preferencias sexuales. Las violaciones a esta disposición, según el artículo 127 de la ley, señala que tiene como sanción el pago de una multa que va de $332.52 a $1'064,044.07, quedando la fijación del monto al arbitrio de la Procuraduría Federal de Protección al Consumidor.

---

[317] En el 2005, Profeco, de forma conjunta con otras agencias gubernamentales, sector académico y privado, revisaron un total de 601 spams. De total de los *spams* que circulan en México, los más comunes pertenecen a las siguientes categorías: I) venta de software y equipo de cómputo, ii) venta de planes de negocios o fórmulas de cómo emprender un negocio, iii) oferta de diversos productos (libros, aparatos domésticos, discos compactos), iv) medicamentos para adulto (viagra, cialis, etc), v) propaganda política y religiosa, vi) servicios financieros, vii) contenido para adulto, viii) productos para bajar de peso, ix) joyería, x) lotería y casinos virtuales, entre otros .Cabe destacar que el porcentaje de las primeras cinco categorías sumaron un estimado de 60% del total de los *spams* que circulan en los correos electrónicos mexicanos. Asimismo, las principales faltas a las Directrices de la OCDE fueron las siguientes: datos de contacto incompletos; publicidad engañosa; anuncio de prácticas comerciales abusivas y fraudulentas; contenían información falsa y engañosa. Asimismo, en la mayoría de los casos, la opción para no seguir recibiendo estos mensajes no funciona por lo que el usuario no puede ejercer su derecho de no recibir tales mensajes. Información obtenida de la página de la Procuraduría Federal de Protección al Consumidor, www.profeco.gob.mx

En lo referente a la confidencialidad de la información que es otorgada por los consumidores se encuentra regulada en el artículo 76 bis en su fracción primera:

> I. El proveedor utilizará la información proporcionada por el consumidor en forma **confidencial**, por lo que no podrá **difundirla** o transmitirla a otros proveedores ajenos a la transacción, **salvo** autorización expresa del propio consumidor o por requerimiento de autoridad competente;

La segunda fracción impone obligaciones tendientes al empleo por parte de proveedores de medidas que garanticen la seguridad y confidencialidad de la información que proporcionan los consumidores:

> II. El **proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información** proporcionada por el consumidor e informará a éste, **previamente** a la celebración de la transacción, de las características generales de dichos elementos;

Aunque en la realidad esto no sucede. La mayoría de los sitios que asegura proveer de medios eficaces para la protección de los datos personales, nos engaña. Basta leer las políticas de privacidad de varios sitios radicados en nuestro país y nos daremos cuenta de la arbitrariedad de los proveedores y su desden en hacer cumplir la ley.[318]

Es importante destacar la labor que ha hecho en estos últimos años la Procuraduría Federal de Protección al Consumidor en el tratar de evitar el *spam*, una de las formas de atentar contra la vida privada en Internet.

Profeco participó en el panel intitulado "Protección de datos personales: privacidad y mecanismos anti-spam" del 4º Encuentro Estratégico de Internet 2004, celebrado los días 28 y 29 de septiembre de 2004 en la Ciudad de México. El Encuentro fue organizado por la Asociación Mexicana de Internet (AMIPCI). La institución enfatizó las actividades nacionales e internacionales que lleva a cabo a efecto de combatir el *spam* y salvaguardar la privacidad de los ciberconsumidores. Se mencionó que la Ley Federal de Protección al Consumidor contiene cláusulas relativas al comercio electrónico y a la privacidad de los datos personales. El Foro "*Spam* y su Impacto" organizado por la Facultad de Derecho de la Universidad La Salle y la Comisión Federal de Telecomunicaciones (Cofetel), se celebró los días 3 y 4 de marzo de 2005 en la Ciudad de México. En dicho foro Profeco impartió dos ponencias relativas a temas como: "La necesaria coordinación entre autoridad, industria y sociedad en el control del *spam*" y "El combate *anti-spam* en el marco internacional y los foros internacionales especializados". La temática tratada fue diversa: qué es el *spam* y por qué existe; efectos negativos de éste sobre la infraestructura

---

[318] Veamos como ejemplo un apartado de las políticas de privacidad del sitio www.despegar.com.mx, que proveo de paquetes vacacionales: "**Seguridad**: Esta página contiene medidas de seguridad para protección contra pérdida, uso indebido, o alteración de la información, bajo control de Despegar.com. Estas medidas de seguridad incluyen el uso de codificación SSL (*Secure Socket Layer*) que es un sistema que permite a su *browser* codificar automáticamente los datos antes de enviarlos a Despegar.com. A pesar de nuestras medidas de seguridad, le rogamos tener en cuenta que la "seguridad perfecta" no existe en Internet." Es una buena excusa o tal vez es una salida fácil.

informática; el *spam* y los virus informáticos; el *spam* desde una perspectiva comercial; perspectiva de la industria en el combate al *spam*; el *spam* en el contexto de los delitos cibernéticos y el *spam* dentro del ámbito de la organización en Internet. Por último participó en el "Foro *spam* y sus perspectivas de solución" organizado por la Comisión de Comunicaciones de la Cámara de Diputados que se llevó a cabo el 28 de junio de 2005 en la Ciudad de México. En este encuentro Profeco presentó una ponencia intitulada "Combate *antispam* en el marco internacional y de los foros internacionales especializados" en donde se mencionó cuáles son las acciones nacionales e internacionales de Profeco a efecto de combatir el *spam*, las mejores prácticas internacionales a efecto de combatir este fenómeno y cuáles son los foros internacionales en donde Profeco participa en la discusión del tema. Foros todos interesantes que nos dotaron de mucho material y por su extensión serían materia de un nuevo estudio.

Para finalizar lo que dice De Miguel Asensio[319] es el sentir personal: "La LFPC no establece un régimen elaborado de protección de datos personales que imponga a los responsables del tratamiento obligaciones o atribuya a los particulares derechos semejantes a los previstos en la normativa de la Unión Europea. Por ello México en la actualidad es considerado desde la UE como un país que no ofrece un nivel de protección adecuado." De esta forma parece que nuestro país tiene una tarea importante que realizar para integrarse a los procesos económicos que envuelve la Unión Europea y por lo tanto estar en situación de competencia frente a los países que la integran.

13.- Ley Federal de Telecomunicaciones

Esta ley publicada en el Diario Oficial de la Federación el 7 de junio de 1995, tiene como principal objeto el regular el uso, aprovechamiento y explotación del espectro radioeléctrico, de las redes de telecomunicaciones y de la comunicación vía satélite. Ha tenido una única reforma publicada en el Diario Oficial de la Federación el 11 de abril del 2006, mismas que han sido muy polémicas y criticadas por varios sectores de la sociedad, basta citar lo que nos dice Clara Luz Álvarez González de Castilla:[320] "las Reformas restan facultades al gobierno mexicano para ejercer su rectoría sobre el espectro radioeléctrico, pueden distorsionar de manera importante el mercado de telecomunicaciones y omiten fortalecer a la Cofetel para que esta pueda cumplir oportunamente su mandato". Si bien es cierto este tema no nos compete, también lo es que resulta de interés para cualquier estudioso del derecho. En función a la protección a la vida privada, el artículo 49 del mencionado ordenamiento nos dice:

---

[319] Op. Cit. pág. 176.

[320] ÁLVAREZ GONZÁLEZ DE CASTILLA, Clara Luz, ***Análisis a las reformas de la Ley Federal de Telecomunicaciones*** en ***Reforma de medios electrónicos. ¿Avances o retrocesos?,*** HUBER, Rudolf, VILLANUEVA, Ernesto (coords.) UNAM, Instituto de Investigaciones Jurídicas, 2007, pág. 101.

> **Artículo 49.** La información que se transmita a través de las redes y servicios de telecomunicaciones será confidencial, salvo aquella que, por su propia naturaleza, sea pública, o cuando medie orden de autoridad competente.[321]

El numeral citado establece la confidencialidad que debe existir en la transmisión de información a través de redes y servicios del espectro radioeléctrico. Con su respectiva excepción en el caso que la información sea pública o exista orden de autoridad competente. Ilustra de forma sencilla el principio que hemos estudiado, donde se privilegian los derechos de la mayoría al tratarse de cosas relacionadas al interés público.

14.- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

La primera aproximación en materia de protección de datos personales se dio con la aprobación de este cuerpo legal. La alusión que realiza esta legislación en lo referente a los datos personales es de forma y no de fondo. Este cuerpo legal tiene como finalidad proveer lo necesario para garantizar el acceso a toda persona a la información en posesión de los poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal, pero a la vez garantiza la protección de los datos personales que obran en los Poderes Ejecutivo, Legislativo y Judicial. Es una ley que tiene un ámbito de aplicación federal, por lo que cada entidad federativa ha creado su propia ley, y como ya referimos anteriormente, con la reciente iniciativa de reforma al artículo 6º constitucional, se busca fijar una serie de parámetros aplicables a todas las entidades federativas.

Un concepto trascendente, ya analizado, es el que la LFTAIPG, señala resepcto lo que son los datos personales contemplado en su artículo 3º fracción II:

> **Artículo 3.** Para los efectos de esta Ley se entenderá por:
>
> **II. Datos personales:** La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad;[322]

Claro que estos datos únicamente están tutelados si se encuentran en posesión de cualquiera de los órganos gubernamentales que ya enumeramos. Consideramos que esta es la definición legal de los mismos en nuestro país.

Este ordenamiento también consagra la confidencialidad de los datos personales:

---

[321] ***Ley Federal de Telecomunicaciones***, Cámara de Diputados, Reformas publicadas al 11 de abril de 2006, http://www.diputados.gob.mx/LeyesBiblio/doc/118.doc

[322] ***Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/244.doc

Artículo 18. Como **información confidencial se considerará**:

I. La entregada con tal carácter por los particulares a los sujetos obligados, de conformidad con lo establecido en el Artículo 19, y

II. Los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta Ley.

No se considerará confidencial la información que se halle en los registros públicos o en fuentes de acceso público.

Artículo 19. Cuando los particulares entreguen a los sujetos obligados la información a que se refiere la fracción I del artículo anterior, deberán señalar los documentos que contengan información confidencial, reservada o comercial reservada, siempre que tengan el derecho de reservarse la información, de conformidad con las disposiciones aplicables. En el caso de que exista una solicitud de acceso que incluya información confidencial, los sujetos obligados la comunicarán siempre y cuando medie el consentimiento expreso del particular titular de la información confidencial.

Al decir de Reyes Krafft:[323] "Los datos de las personas que obran en las instituciones públicas son confidenciales y, por lo tanto, no deben divulgarse ni utilizarse con fines distintos para los cuales fueron recibidos o requeridos, de tal manera que se garantice el derecho a la intimidad y la vida privada, y al mismo tiempo sus titulares deben tener acceso a ellos cuando lo soliciten." Este es un principio que tiene como intención proteger a las personas y como dijera Ríos Estavillo:[324] "Se ha insistido que el derecho de acceso resguarda límites, entre ellos la confidencialidad y el secreto de reserva, los cuales se justifican por razones de interés público como por razones de interés privado."

Este ordenamiento garantiza el derecho de las personas a la vida privada, al obligar a las instituciones a proteger los datos personales que tienen en sus archivos o bases de datos. En su Capítulo IV "Protección de Datos Personales incluye una serie de disposiciones importantes en la materia:

Artículo 20. Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:
VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

En este numeral encontramos la obligación de lealtad, así denominada por Ovilla Bueno[325] que consiste en la prohibición de la comercialización de los datos.

Artículo 21. Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.

---

[323] REYES KRAFFT, Alejandro, ***Protección de Datos Personales en México. Génesis Legislativa***, Revista de Derecho Informático, No. 100, Noviembre 2006, http://www.alfa-redi.org/rdi-articulo.shtml?x=7846
[324] RÍOS ESTAVILLO, Juan José, ***Derecho a la Información en México***, Editorial Porrúa, México, 2005, pág. 153
[325] OVILLA BUENO, Rocío, Op. Cit. pág. 40.

Además cualquier persona puede solicitar ante las Unidades de Enlace de las dependencias y entidades, información sobre sus datos personales.

> **Artículo 24.** Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales. Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante.

O en su caso cualquier persona podrá solicitar por sí o por medio de su representante legal a las Unidades de Enlace de las dependencias y entidades, la modificación de sus datos en el sistema de datos de que se trate.

> **Artículo 25.** Las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales. Con tal propósito, el interesado deberá entregar una solicitud de modificaciones a la unidad de enlace o su equivalente, que señale el sistema de datos personales, indique las modificaciones por realizarse y aporte la documentación que motive su petición. Aquélla deberá entregar al solicitante, en un plazo de 30 días hábiles desde la presentación de la solicitud, una comunicación que haga constar las modificaciones o bien, le informe de manera fundada y motivada, las razones por las cuales no procedieron las modificaciones.

A nuestro modo de ver, no se trata de un habeas data propiamente dicho, por las explicaciones que dimos al respecto en el capítulo primero de este trabajo, a pesar que el Comisionado del Instituto Federal de Acceso a la Información Pública, Horacio Aguilar Álvarez de Alba[326] dijera en su conferencia presentada el 27 de septiembre de 2006, en el Seminario Internacional de Acceso a la Información Judicial y Nuevas Tecnologías.

Esta ley crea lo que se ha denominado el "Sistema Persona"[327] el cual se establece para dar cumplimiento a lo dispuesto por los artículos 23 de la ley y 48 de su reglamento, constituye un registro de los sistemas de datos personales, que son el conjunto ordenado de datos personales en posesión de una dependencia o entidad, con independencia de su forma de acceso, creación, almacenamiento u organización, pueden ser físicos o automatizados incluyendo las modificaciones y transmisiones de los mismo y se actualiza de manera semestral. Para darnos una idea de la cantidad de datos que de nosotros posee el Gobierno Federal, tomaremos algunos datos de la ponencia titulada "Nuevas tecnologías en materia de acceso a la información y protección de datos personales" impartida por el Comisionado del IFAI, Juan Pablo

---

[326] AGUILAR ÁLVAREZ DE ALBA, Horacio, ***La Protección de Datos Personales en México***, 27 de septiembre de 2006, Suprema Corte de Justicia de la Nación, http://200.38.86.53/NR/rdonlyres/268296FA-DE64-441C-91E1-888A72C3A035/0/presentaciondedatospersonales26deseptiembrevfppt.pdf

[327] Para mayor información consultar el sitio del **Sistema Persona** en el IFAI: http://persona.ifai.org.mx También es necesario revisar los ***"Lineamientos de Protección de Datos Personales"*** publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005.

Guerrero Amparán:[328] El primer registro en "Persona" se realizó en marzo de 2006 y su primera actualización en septiembre de 2006, se han registrado 1865 sistemas de datos personales por 179 dependencias y entidades de los cuales 796 son en medios físicos, 1001 en medios automatizados y 68 cuentan con respaldo físico y automatizado.

Esta Ley crea el Instituto Federal de Acceso a la Información Pública Gubernamental (IFAI),[329] el Decreto que lo crea es publicado en el Diario Oficial de la Federación el 24 de diciembre de 2002, entre sus funciones están:

1) Garantizar el derecho de acceso a la información pública gubernamental
2) Proteger los datos personales que están en manos del gobierno federal
3) Y resolver sobre las negativas de acceso a información que las dependencias o entidades del gobierno federal hayan formulado

A partir de la entrada en vigor de la Ley de Transparencia y Acceso a la Información Pública Gubernamental, más de 250 dependencias y entidades del gobierno federal tienen la obligación de atender las solicitudes de información. Todas ellas abrirán una Unidad de Enlace para ese fin. Una vez solicitada, un Comité de Información en cada dependencia determinará si la información se otorga o no. En caso de que la decisión sea negativa, el solicitante puede interponer un recurso de revisión ante el IFAI. El IFAI sólo interviene en aquellos casos en los cuales, las personas se inconformen e interpongan un recurso de revisión. El IFAI elaborará un dictamen en cada caso, abriendo la información o confirmando la decisión de la dependencia. En cualquier caso, el IFAI trabajará bajo el principio de publicidad de la información del gobierno. El IFAI es un organismo descentralizado de la Administración Pública Federal, no sectorizado, y goza de autonomía operativa, presupuestaria y de decisión. El IFAI para cumplir con su obligación de proteger los datos personales cuenta con la Dirección General de Clasificación y Datos Personales, misma que tiene su sustento legal en el artículo 6º del Reglamento Interior del IFAI y que según opinión de Aveleyra podría convertirse en la autoridad para regular los datos personales que manejan particulares, en lugar de crear un nuevo Instituto. Podemos decir que el Instituto ha entregado buenas cuentas, se han interpuesto en materia de datos personales, 483 recursos revisión desde el 12 de junio de 2003 al 31 de agosto de 2006, implicando un 6.9% del universo de recursos de revisión interpuestos, en cuanto a solicitudes de información de datos personales al 18 de septiembre de 2006 se han acumulado 15,303 solicitudes de acceso y corrección de datos.[330]

---

[328] GUERRERO AMPARÁN, Juan Pablo, ***Nueva tecnologías en materia de acceso a la información y protección de datos personales***, Suprema Corte de Justicia de la Nación, http://200.38.86.53/NR/rdonlyres/178A09DC-CE5B-4AD6-AFB6-62ECAD9D3F8D/0/IFAIJPGADPTecnologias26sep06ppt.pdf

[329] Podemos decir que según Marcia Muñoz de Alba el antecedente del IFAI esta en la primera ley federal alemana para la protección contra el abuso de datos sobre las personas con motivo del tratamiento electrónico de los mismos, documento en el que se crea la figura de un funcionario encargado de velar por el cumplimiento de la ley, esta entro en vigor el 1º de enero de 1970 adoptada por el *Land de Hesse*. Otro referente podría ser la ley francesa relativa a la informática, los ficheros y la libertad de 6 de enero de 1978 que crea la Comisión Nacional de Informática y Libertades con facultades reglamentarias, de control y protección al público en materia de recolección de datos. MUÑOZ DE ALBA MEDRANO, Marcia, ***Habeas Data*** en ***Estudios en homenaje a Marcia Muñoz de Alba Medrano. Estudios de Derecho Público y Política***, CIENFUEGOS SALGADO, David y MACÍAS VAZQUEZ, María del Carmen (coords.) UNAM, Instituto de Investigaciones Jurídicas, México, 2006, pág. 6.

[330] En GUERRERO AMPARÁN, Juan Pablo, Op. Cit.

Es oportuno señalar que la implementación y operación de la ley ha tenido éxito, los ciudadanos han podido obtener información del quehacer gubernamental y además han logrado tener acceso a su información.[331] Pero existen puntos oscuros en la misma, ya que por es imprecisa con relación a la facultad del IFAI para ordenar la entrega de información confidencial, puede interpretarse que el IFAI favorece el principio de máxima publicidad y ordene la entrega cuando dicho principio quede por encima del derecho a la privacidad. Por otra parte la Ley no prevé la valoración del prejuicio al derecho a la privacidad, frente al beneficio social del acceso.

15.- Ley Federal del Derecho de Autor

Esta ley reglamentaria del artículo 28 constitucional, publicada en el Diario Oficial de la Federación el 24 de diciembre de 1996, tiene por objeto la protección de los derechos de los autores de toda obra intelectual o artística y la salvaguarda del acervo cultural de la nación. Esta legislación también contempla la protección de la vida privada de las personas, sobre todo el derecho a la imagen propia y el nombre. El numeral 188 contiene varias disposiciones interesantes:

> **Artículo 188.-** No son materia de reserva de derechos:
>
> **I. Los títulos, los nombres, las denominaciones, las características físicas o psicológicas,** o las características de operación que pretendan aplicarse a alguno de los géneros a que se refiere el artículo 173 la presente Ley, cuando:
>
> **e) Incluyan el nombre, seudónimo o imagen de alguna persona determinada, sin consentimiento expreso del interesado**, o
>
> **VII. Los nombres de personas utilizados en forma aislada**, excepto los que sean solicitados para la protección de nombres artísticos, denominaciones de grupos artísticos, personajes humanos de caracterización, o simbólicos o ficticios en cuyo caso se estará a lo dispuesto en el inciso e) de la fracción I de este artículo, y[332]

Entonces el nombre, seudónimo, imagen de alguna persona determinada, sin consentimiento expreso del interesado, no constituyen materia de derechos de autor, infraccionando (artículo 231, II) cuando se utilice la imagen de una persona sin su autorización o la de sus causahabientes.

Por otra parte, también se contempla la protección jurídica de las bases de datos, misma que no se extiende a los datos y materiales en sí mismos.

> **Artículo 107.-** Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como

---

[331] Los logros en materia de acceso a la información pueden ser consultados en los informes que el IFA presenta al H. Congreso de la Unión publicados en el sitio de Internet del IFAI: http://www.ifai.org.mx/rendicion/rendicion.php

[332] ***Ley Federal del Derecho de Autor***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/122.doc

> compilaciones. **Dicha protección no se extenderá a los datos y materiales en sí mismos.**

El acceso a la información de carácter privado relativa a las personas contenida en las bases de datos,[333] así como su publicación, reproducción, divulgación, comunicación publica y transmisión de dicha información, requerirá la autorización previa de los ciudadanos de que se trate.

> **Artículo 109.- El acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.** Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

Existe entonces protección a las personas en este ordenamiento legal, partiendo del supuesto de la imagen y la pertenencia de características físicas y psicológicas propias.

Un tema que me parece muy interesante, tal vez por mi vinculación laboral con los indígenas es aquel que aborda Carlos Viñamata donde nos señala los derechos que tienen los indígenas de recibir un pago por cada foto, cuadro obra, grabado, pintura o cualquier manera en que se difunda su imagen, siendo esta una forma de preservar la cultura popular y que la misma genere beneficios, pues entonces se hará la prolífica y beneficiará a sus creadores e interpretes. Así por solo poner un ejemplo: "...se pueden proteger los nombres de las diversas etnias como nombres de dominio en Internet, asegurando con ello una protección, una exclusividad y una proyección del nombre reservado a nivel mundial."[334]

16.- Ley General de Población

Esta ley es publicada en el Diario Oficial de la Federación el 7 de enero de 1974, tiene como objeto regular los fenómenos que afectan a la población en cuanto a su volumen, estructura, dinámica y distribución en el territorio nacional. En primer lugar establece la obligación de todos los mexicanos, de inscribirse en el Registro Nacional de Población, dependiente de la Secretaria de Gobernación:

> **Artículo 98.-** Los ciudadanos mexicanos tienen la obligación de inscribirse en el Registro Nacional de Ciudadanos y obtener su Cédula de Identidad Ciudadana.

---

[333] Al respecto ver OVILLA BUENO, Rocío, ***La protección jurídica de las bases de datos en México. De los lineamientos internacionales a la Nueva Ley Federal del Derecho de Autor*** en ***Estudios de Derecho Intelectual en homenaje a David Medina Rangel,*** Becerra Ramírez Manuel (compilador), UNAM, Instituto de Investigaciones Jurídicas, México, 1998, págs. 297-321

[334] VIÑAMANTA PASCHKES, Carlos, ***Indigenismo y Propiedad Intelectual,*** Editorial Porrúa, México, 2006, pág. 176.

Al ser parte de este registro se nos va a asignar una Clave Única de Registro de Población, como lo señala el artículo 91. Para instrumentarla, se publica el 22 de Octubre de 1996 el Acuerdo Presidencial que ordena la Adopción y Uso por la Administración Pública Federal de la CURP[335]. La CURP es un número único de identificación, pero que permite, por sus solas características, identificar a la persona de que se trata, junto con una serie de sus datos personales, lo cual se obtiene por su forma de composición.

17.- Ley General de Salud

Esta ley reviste especial importancia ya que el bien jurídicamente tutelado es la vida. Los ciudadanos tienen muchos derechos en cuanto a información clínica se refiere, pueden recibir toda la información suficiente, clara oportuna y verídica así como la orientación que sea necesaria respecto a como atender algún problema de salud; se tiene la obligación de conservar los expedientes clínicos en las instituciones de salud; el contar con un expediente clínico y el más importante y que encuadra en la protección a la vida privada: el que el trato que se le de al paciente sea confidencial.

> **Artículo 77 bis 37**.- Los beneficiarios del Sistema de Protección Social en Salud tendrán además de los derechos establecidos en el artículo anterior, los siguientes:
> I al IX
> **X.** Ser tratado con confidencialidad.[336]

Es importante destacar el dato que aporta Gómez Robledo, al respecto de los datos contenidos en los servicios de salud que obtuvo de un análisis del XII Censo General de Población y Vivienda 2000: "...los beneficiarios estaban distribuidos de acuerdo con la institución que los atiende, de la siguiente manera: 39% son atendidos en instituciones de seguridad social, 34% por servicios médicos privados, y otro 26% es atendido por servicios a la población abierta, de modo que más de la mitad son atendidos por instituciones particulares que no están vinculadas a la LAI y por tanto no son sujetos obligados de su capítulo referente a la protección de datos personales."[337] De la

---

[335] La clave contiene 18 elementos de un código alfanumérico. De ellos, 16 son extraídos del documento probatorio de identidad de la persona (acta de nacimiento, carta de naturalización, documento migratorio o certificado de nacionalidad mexicana), y los dos últimos los asigna el Registro Nacional de Población.
Ejemplo hipotético: Alamán Pérez Ricardo, nació en el D.F. el 21 de marzo de 1963

- Del primer apellido, primera letra y primera vocal interna (AA).
- Del Segundo apellido, primera letra (P). En caso de no tener segundo apellido se posiciona una "X"
- Del primer nombre, primera letra (R). En nombres compuestos que comiencen con María o José, se tomará en cuenta el segundo nombre para la asignación de la inicial.
- De la fecha de nacimiento, año, mes y día (630321).
- Del sexo, (H) para hombre y (M) para mujer. En este caso hombre (H).
- Del lugar de nacimiento, las dos letras según el código de la Entidad Federativa que corresponda (DF).
- De los apellidos y primer nombre, las primeras consonantes internas de cada uno (LRC).
- La posición 17 es un carácter asignado por el Registro Nacional de Población para evitar registros duplicados (0).
- El último es un dígito verificador, un número que también es asignado por el Registro Nacional de Población (6).

Información obtenida de la página de preguntas frecuentes sobre el CURP, en el sitio de la Secretaría de Gobernación: http://www.segob.gob.mx/templetas/blank.php?idCont=182

[336] ***Ley General de Salud***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/142.doc

[337] GÓMEZ ROBLEDO, Alonso, ORNELAS NÚÑEZ, ***Protección de Datos Personales en México: El caso del Poder Ejecutivo Federal***, Instituto de Investigaciones Jurídicas, UNAM, México, 2007, pág. 27.

lectura de las cifras narradas, se hace cada vez más necesaria la regulación y tratamiento de los datos personales en la esfera del mundo privado, ya que muchas organizaciones de salud tienen estos datos y pueden hacer mal uso de los mismos ya que no existe ninguna regulación al respecto.

Por último cabe mencionar que la Norma Oficial Mexicana, 168-SSA1-1998, que establece los criterios científicos, tecnológicos y administrativos obligatorios en la elaboración, integración, uso y archivo del expediente clínico, en su punto número 5 señala:

> **5.6.** En todos los establecimientos para la atención médica, la información contenida **en el expediente clínico será manejada con discreción y confidencialidad**, atendiendo a los principios científicos y éticos que orientan la práctica médica y sólo podrá ser dada a conocer a terceros mediante orden de la autoridad competente, o a CONAMED, para arbitraje médico.[338]

Reiterando la confidencialidad y discreción sobre la información contenida en el expediente clínico y únicamente podrá ser dado a conocer mediante orden de autoridad competente.

18.- Ley para Regular las Sociedades de Información Crediticia

Esta ley se crea en función de la necesidad del mercado de contar con instituciones que procesen los datos sobre el comportamiento del crédito de las personas, físicas y morales, publicada en el Diario Oficial de la Federación el 15 de enero de 2002. Al decir de Gómez-Robledo: "Estamos ante un caso en el cual la privacidad se subordina a la necesidad del mercado de conocer el riesgo de insolvencia de una persona física, permitiendo su divulgación a una persona distinta del titular de los datos personales (institución de crédito, tienda de autoservicio, compañía de telefonía etcétera)".[339] Se tiene que mencionar que dicho ordenamiento prevé una protección a datos tan sensibles.

> **Artículo 22.**- La Sociedad deberá adoptar las **medidas de seguridad y control que resulten necesarias para evitar el manejo indebido de la información**.
>
> Para efectos de esta ley, **se entenderá** por uso o manejo indebido de la información cualquier acto u omisión que cause daño en su patrimonio, al **sujeto** del que se posea información, así como cualquier acción que se traduzca en un beneficio patrimonial a favor de los funcionarios y empleados de la Sociedad o de esta última, siempre y cuando no se derive de la realización propia de su objeto.[340]

Deben estas sociedades garantizar la protección de la información, tomando las medidas de seguridad necesarias para evitar el mal manejo de la misma.

> **Artículo 18.**- A las Sociedades les estará **prohibido**:
>
> **I. Solicitar y otorgar información distinta a la autorizada conforme a esta ley** y a las demás disposiciones aplicables;

---

[338] ***NOM 168-SSA1-1998. Del expediente clínico***, Secretaría de Salud, http://www.salud.gob.mx/unidades/cdi/nom/168ssa18.html

[339] GOMEZ ROBLEDO, Alonso, Op. Cit. pág. 21.

[340] ***Ley para Regular las Sociedades de Información Crediticia***, Cámara de Diputados, http://www.cddhcu.gob.mx/LeyesBiblio/pdf/237.pdf

Las sociedades de información crediticia tienen prohibido solicitar y otorgar información diferente a la que la ley les autoriza, en este orden de ideas, la ley les permite conocer datos como el nombre, domicilio, teléfono, fecha de nacimiento, créditos que se le han otorgado entre otros, por lo tanto hacer referencia a información distinta a la anterior sería la información no solicitada, por ejemplo ideología, predilección sexual, estado de salud, religión entre otros.

> **Artículo 28.-** Las Sociedades sólo podrán proporcionar información a un Usuario, cuando éste cuente con la autorización expresa del Cliente, mediante su firma autógrafa, en donde conste de manera fehaciente que tiene pleno conocimiento de la naturaleza y alcance de la información que la Sociedad proporcionará al Usuario que así la solicite, del uso que dicho Usuario hará de tal información y del hecho de que éste podrá realizar consultas periódicas de su historial crediticio, durante el tiempo que mantenga relación jurídica con el Cliente.

Dentro del marco de esta ley se crea la empresa privada Buró de Crédito, que hoy por hoy es la sociedad de información crediticia más importante en el país. Su base de datos de personas físicas esta formada por 94.9 millones de registros al 31 de enero de 2007, y 6.1 millones de registros de personas morales.[341] Estas cifras nos hablan de la cantidad de datos que fluyen en estas sociedades crediticias y por ende la importancia que reviste la regulación más oportuna de estas cantidades de información.

19.- Ley Reglamentaria del Artículo 5º Constitucional, Relativo al Ejercicio de Profesiones en el Distrito Federal.

Esta legislación regula la forma en que se deben ejercer las profesiones que requieren título para su ejercicio. Y contempla lo que se conoce como el secreto profesional. Al decir del maestro Humberto Quiroga:[342] "Se entiende por "secreto" aquello que "se tiene reservado y oculto cuidadosamente". Sin embargo, el concepto de "secreto profesional" es más amplio porque incluye también, aquello que aun no siendo de conocimiento por parte de su titular, su revelación pueda causarle daño. La doctrina nacional y extranjera tiene especificado el concepto del secreto profesional como "todo aquello que se confíe al profesional bajo la condición de su divulgación". Así la legislación de profesiones que es reglamentaria al artículo 5º constitucional, establece lo siguiente:

> **ARTICULO 36.-** Todo profesionista estará obligado a guardar estrictamente el secreto de los asuntos que se le confíen por sus clientes, salvo los informes que obligatoriamente establezcan las leyes respectivas.[343]

Es de llamar la atención que esta legislación según el artículo 7º rige en el Distrito Federal para asuntos de orden común y para toda la República en asuntos de orden federal, fue publicada en el Diario Oficial de la Federación el 26 de mayo de 1945. Encontramos en otras entidades federativas leyes de

---

[341] Información obtenida de la página de Internet de ***Buró de Crédito***, http://www.burodecredito.com.mx/index.htm

[342] QUIROGA LAVIÉ, Humberto, ***La protección de la intimidad y la regulación del secreto*** en ***Derecho a la información y derechos humanos***, CARPIZO, Jorge y CARBONELL, Miguel (coords.) UNAM, Instituto de Investigaciones Jurídicas, México, 2000, pág. 503.

[343] ***Ley Reglamentaria del Artículo 5º Constitucional, Relativo al Ejercicio de Profesiones en el Distrito Federal***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/208.doc

profesiones que tienen jurisdicción dentro de su territorio como es el caso de la legislación de Durango, que también contempla como obligación del profesionista el guardar el secreto profesional (Ley Para el Ejercicio de las Profesiones en el Estado de Durango, artículo 16 fracción III)

20.- Ley Sobre Delitos de Imprenta

La Ley de Imprenta de 1917 en su artículo 1º expresa lo que se constituye como un ataque a la vida privada pero es concebido como manifestaciones maliciosas hechas en forma verbal por un medio manuscrito, o la imprenta o cualquier manera que expuesta o circulando en público, por correo, telégrafo, etcétera cause demérito en su reputación o sus intereses:

> **Artículo 1o.-** Constituyen ataques a la **vida privada**:
>
> I.- Toda **manifestación o expresión maliciosa hecha verbalmente o por señales en presencia de una o más personas, o por medio de manuscrito, o de la imprenta, del dibujo, litografía, fotografía o de cualquier otra manera que expuesta o circulando en público, o transmitida por correo, telégrafo, teléfono, radiotelegrafía o por mensajes, o de cualquier otro modo,** exponga a una persona al odio, desprecio o ridículo, o pueda causarle demérito o en su reputación o en sus intereses;
>
> II.- Toda manifestación o expresión maliciosa hecha en los términos y por cualquiera de los medios indicados en la fracción anterior, contra la memoria de un difunto con el propósito o intención de lastimar el honor o la pública estimación de los herederos o descendientes de aquél, que aún vivieren;
>
> III.- Todo informe, reportazgo o relación de las audiencias de los jurados o tribunales, en asuntos civiles o penales, cuando refieran hechos falsos o se alteren los verdaderos con el propósito de causar daño a alguna persona, o se hagan, con el mismo objeto, apreciaciones que no estén ameritadas racionalmente por los hechos, siendo éstos verdaderos;
>
> IV.- Cuando con una publicación prohibida expresamente por la Ley, se compromete la dignidad o estimación de una persona, exponiéndola al odio, desprecio o ridículo, o a sufrir daños o en su reputación o en sus intereses, ya sean personales o pecuniarios.[344]

Creemos que vida privada es el término correcto a utilizar, ya que tanto la Constitución como esta legislación hablan de la vida privada, si bien como ya lo estudiamos, no existe un concepto claro, por interpretación sistemática podemos obtener un acercamiento al mismo.

Existe una gran polémica dentro de la doctrina[345] sobre la validez de esta ley. Estamos frente a una norma previa a la entrada en vigor de la Constitución Política de 1917. Ya que en abril de 1917, Venustiano Carranza, expidió la Ley de Imprenta que rige actualmente, lo que ha generado problemas de eficacia normativa en virtud de que en la práctica no se obedece. La Ley de Imprenta

---

[344] ***Ley Sobre Delitos de Imprenta,*** Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/40.doc

[345] Entre otros VILLANUEVA, Ernesto, ***Derecho mexicano de la información,*** Oxford, México, 2000, pág. 13. o CARPIZO, Jorge, ***"Constitución e información"***, en CARBONELL Y VALADES (coords.), ***Constitucionalismo iberoamericano del siglo XXI,*** UNAM, Instituto de Investigaciones Jurídicas, México, 2000, pág. 42.

de Carranza sigue aplicándose en la actualidad con el auspicio de la Suprema Corte de Justicia, que considera que la legislación preconstitucional tiene fuerza legal en tanto no vaya en contra de la Constitución en vigor y no haya sido derogada. La opinión del Maestro Burgoa[346] en relación a lo anterior es contundente: "...estimamos jurídicamente hablando no debe tener vigencia. En efecto, dicha legislación entró en vigor el día 5 de abril de 1917, esto es, antes de la Constitución de 1917, cuyos artículos 6º y 7º pretende reglamentar. Este ordenamiento fundamental, que rige desde el primero de mayo de 1917, propiamente es una ley posterior a la de abril de dicho año, por lo que derogó a ésta. Además, una reglamentación como es lo que pretende establecer la Ley de Imprenta de don Venustiano Carranza, no tiene razón de ser si no están vigentes los preceptos reglamentados o por reglamentarse: y como estos, es decir, los artículos 6 y 7 entraron en vigor posteriormente, luego no pudieron haber sido objeto de una ley orgánica de anterior vigencia. Sin embargo y pese al anterior argumento, que podría parecer una sutileza, suele sostenerse la vigencia actual de la Ley de Imprenta."

III.- La protección de datos personales desde la perspectiva de los Órganos Jurisdiccionales.

La información judicial presenta la conflictiva relacionada a la protección de datos personales, abierta en dos dimensiones muy claras, por un lado la administración de recursos y la generación de políticas institucionales y la otra relativa al tratamiento de los datos que, como "Administradora de información pública y privada", adquiere y genera en el ejercicio de su función jurisdiccional.

Los que integramos la administración de justicia, enfrentamos el reto de poder hacer efectivo el derecho de acceso a la información vinculado al principio de publicidad y por otra parte respetar el derecho a la vida privada de las personas en el universo de información que genera la administración de justicia. Esta actividad hace que se recoja y procesen datos, y como consecuencia, genere gran cantidad de información, la cual, en una importante proporción está relacionada a personas determinadas, misma que no puede ser monopolizada, pero tampoco puede ser del todo publicitada, la proyección más radicalizada, derivada de esta visión, habla de un derecho de penetración a la información sin limitaciones; sin embargo aun los más fuertes defensores del libre acceso están convencidos de que éste no se puede realizar sin limitaciones; ésa al decir de Michael Vivant[347] no podría ser una visión realista.

Para darnos algo de luz, es importante señalar lo que la *Information Industry Association* de Estados Unidos, tratando los "principios y políticas de acceso a la información de gobierno", ha dicho: "Los ciudadanos tienen derecho a tener acceso a la información mantenida por entes de gobierno, la cual sólo podría ser restringida mediante una ley especialmente dirigida a reglamentar la

---

[346] BURGOA ORIHUELA, Ignacio, ***Diccionario de Derecho Constitucional, Garantías y Amparo***, Editorial Porrúa, México, 2005, pp. 438-439.

[347] Citado por CONSENTINO, Guillermo, ***La Información Judicial es Pública*** en CABALLERO JUÁREZ, José Antonio y GREGORIO, Carlos, (editores) ***El acceso a la información Judicial en México: una visión comparada***, Instituto de Investigaciones Jurídicas UNAM, México, 2005, pág. 251.

necesaria protección de ciertos y específicos intereses legítimos tales como la privacidad". En este orden de ideas aun pese a la apertura que existe en materia de transparencia, el capítulo de información reservada plantea restricciones en materia judicial. El principio de confidencialidad o reserva no debe entenderse a priori como excluyente del acceso a la información, ya que considerarlo así sería poco acertado, porque dentro de las características de los actos jurisdiccionales se encuentra el principio de la administración de justicia a sujetarse rigurosamente a una norma determinada, con independencia y autonomía para la emisión de sus resoluciones mediante un procedimiento revestido de formalidades esenciales adjetivas, lo que se traduce en el debido proceso legal, que tiene como finalidad la restauración del orden jurídico perturbado para que se realicen los alcances del derecho objetivo, de esta forma la ley procesal tutela situaciones de orden público, como ya lo hemos estudiado, de la moral o de las buenas costumbres, tratándose de la materia familiar o penal, e incluso la protección de los secretos industriales o comerciales de las partes, por lo que el juez, como conductor del proceso, puede celebrar la audiencia en forma secreta, dejando constancia de los motivos que lo animaron a realizarla en privado conforme lo señala por ejemplo el artículo 59 del Código de Procedimientos Civiles del Distrito Federal. Esto no debe entenderse como una resistencia a la democratización, ni mucho menos a la transparencia y acceso a la información, sin que lo único que se subraya es el derecho público al acceso a la información judicial frente al derecho de las partes y terceros que necesariamente debe preservar el juzgador y que es inherente al quehacer judicial, en apego irrestricto a la norma jurídica procesal contando con la garantía del derecho a la privacidad y su seguridad jurídica, de esta suerte solo serán materia de emisión de información pública obligatoria aquellos procesos, cuando exista sentencia ejecutoriada.

Retomando el caso Estados Unidos, encontramos que en más de una ocasión los derechos fundamentales de sus ciudadanos, en especial los referentes a la privacidad y la protección de datos personales se han visto violentados con el pretexto de la seguridad nacional, así que el acceso a la información judicial en el vecino país no es tan amplio como podría apreciarse a primera vista, por ejemplo el caso Nixon vs *Warner Communications Inc.*,[348] la Suprema Corte de Justicia de Estados Unidos estableció que el público goza de un derecho derivado del *common law* para tener acceso a los expedientes judiciales, aun cuando el procedimiento no ha sido concluido, atropellando a todas luces el derecho a la vida privada del expresidente Nixon.

Ahora regresando al caso de México y tomando como ejemplo nuestra Suprema Corte de Justicia, que ha vivido un proceso de autonomización e independencia que sigue su marcha, al igual que lo hace esta joven institución de la República donde el que suscribe labora, el Tribunal Superior Agrario, que si bien no se ha logrado todavía una autonomía plena en materia presupuestal, el proceso sigue avanzando y lo mismo sucede en función del acceso a la información pública, la rendición de cuentas y la transparencia en el Poder Judicial, como ejemplo

[348] Nixon vs Warner Communications, Inc. 435 U.S. 539 (1978)

baste un botón, el 26, 27 y 28 de junio de este 2007, se celebró el Seminario Internacional de Acceso a la Información Judicial en el Derecho Constitucional Comparado, [349] además hoy en día se pueden encontrar obras que contienen no sólo resúmenes de los considerandos de las sentencias, sino el cuerpo mismo de sentencias de gran relevancia o de carácter histórico.

En el caso particular del Tribunal Superior Agrario, los justiciables tienen acceso a las sesiones y sus actas, siempre y cuando estás no impliquen un debate para llegar a la resolución de una controversia judicial. Se trata entonces de que las discusiones de los magistrados que integran el Pleno no sean en secreto, sino de cara a la sociedad, circunstancias que permite acotar la corrupción y a la vez, ampliar la legitimidad de la institución.

También como un derecho de transparencia, esta el acceso a las sentencias que causen estado acompañadas en su caso, de todo el expediente que dio origen a la determinación, así de forma regular se prestan expedientes a alumnos de la carrera en derecho para que sean ofrecidos como parte de sus practicas forenses en materia de procedimiento agrario.

En la página de Internet de los Tribunales Agrarios,[350] se puede acceder al historial profesional de jueces y magistrados, su trayectoria e incluso los criterios bajo los cuales fueron ratificados, así como los informes de labores anuales que rinde el Magistrado Presidente.

Ahora bien y a manera de conclusión, el proceso de la transparencia y la apertura del Poder Judicial no pueden ser absolutos. Hay ciertas informaciones que deben permanecer bajo siglo. Como ejemplo, en otras latitudes, lo que se hace público es el cuerpo del expediente y de la sentencia, suprimiendo los nombres de las personas que intervienen, especialmente en casos penales, familiares y los casos donde intervienen menores. También es notorio que un pendiente nacional tanto a nivel local como federal es poner disponible en los sitios de Internet de los poderes judiciales información suficiente para enriquecer la interacción entre el trabajo del juzgador y los distintos sectores de la sociedad.

IV.- Iniciativas de Ley Federal de Protección de Datos Personales.[351]

En este momento se encuentran presentadas ante el Congreso de la Unión, cuatro iniciativas en materia de protección de datos personales, pendientes de su respectivo dictamen y aprobación. Con la aprobación de esta Ley se persiguen varios objetivos:

---

[349] ***Seminario Internacional de Acceso a la Información Judicial en el Derecho Constitucional Comparado,*** http://www.scjn.gob.mx/AvisosPortal/26.htm

[350] **Tribunal Superior Agrario**: www.tribunalesagrarios.gob.mx

[351] Para orientarnos sobre la elaboración de este apartado fueron de extrema utilidad las dos excelentes conferencias que el Dr. Alfredo Reyes Krafft dicto en el Seminario Internacional de Acceso a la Información Judicial y Nuevas Tecnologías celebrado los días 26 y 27 de septiembre de 2006, organizado por la Suprema Corte de Justicia de la Nación, con el título *Protección de datos personales* y disponibles en línea en las siguientes direcciones electrónicas: http://200.38.86.53/NR/rdonlyres/07543784-B096-4D7A-A97B-E671FFF40055/0/DATOSPERSONALESARKSCJNppt.pdf y http://200.38.86.53/NR/rdonlyres/A4D4B97D-850F-4FE5-83E7-7A27886E7602/0/DATOSPERSONALESARKppt.pdf

- La protección de los datos personales que obran en manos de particulares sean personas físicas o morales, no como el régimen actual que únicamente protege estos datos, mientras estén en posesión de los Poderes de la Unión o entidades gubernamentales diversas.
- La distinción de los datos sensibles o los relacionados con la vida privada de otros de tipo público.
- Una legislación para obligar a ponderar entre el perjuicio a la vida privada y el interés público. Es decir, replantear la noción de privacidad, pues la información de millones de personas se encuentra disponible en la red y en las bases de datos privadas.
- Elevar los castigos por el mal uso de los datos personales, lo que implica reconocer la insuficiencia y obsolescencia de las medidas actuales de protección de datos personales, debido a que la información personal fluye por medios electrónicos a velocidades de transmisión y costos irrisorios, que rebasan criterios tradicionales de protección.
- La adecuación y respeto a los Tratados suscritos por México, que protegen la vida privada, estudiados en el anterior apartado.
- Un justo medio entre los intereses de los actores comerciales (publicidad y mercadotecnia) y la protección a la vida privad de forma que no resulte gravoso o una carga excesiva que limite el crecimiento de las empresas que laboran en nuestro país.
- La existencia de medios de defensa, administrativos o judiciales.

Es importante señalar que en las iniciativas que hemos de comentar se contienen principios de protección de datos personales, aplicables al sector privado y público, se prevé la creación de un nuevo Instituto Federal de Protección de Datos Personales, mientras otras manejan que sea el actual IFAI, el encargado, también algunos manejan el sistema *opt out*, entre otras diferencias. Lo que es un hecho es que a pesar de contar con distintas disposiciones jurídicas en materia de datos personales, es un hecho que resulta indispensable reglamentar el tratamiento de datos personales en nuestro país a través de una ley que regule al sector privado a efecto de fijar disposiciones que tomen en cuenta el respecto del derecho a la vida privada y aclare si la comercialización de los datos personales priva sobre el derecho a la vida privada o buscar de una u otra forma la conciliación de ambos intereses. Es un hecho de que cualquier decisión que se tome al respecto tendrá un impacto para los actores económicos involucrados, por lo que un balance será en extremo necesario. Se enumeran por fecha de presentación, no por otra razón en particular.

1.- Iniciativa de Ley Federal de Protección de Datos Personales, presentada por el diputado Jesús Martínez Álvarez del Partido Convergencia, el 1º de diciembre de 2005.[352]

[352] Gaceta Parlamentaria, No. 1895-1, Año. 2005, México D.F. Jueves 1º de diciembre, Cámara de Diputados, ***Iniciativa de Ley Federal de Protección de Datos Personales, presentada por el diputado Jesús Martínez Álvarez del Partido Convergencia, el 1º de diciembre de 2005*** http://gaceta.diputados.gob.mx/Gaceta/59/2005/dic/Anexo-I-01dic.html

Esta iniciativa es publicada en la Gaceta Parlamentaria número 1895-I del jueves 1 de diciembre de 2005, fue turnada a la Comisión de Gobernación para su dictamen, no ha sido aprobada por la Cámara de Diputados, tampoco por la de Senadores y menos aun su publicación en el Diario Oficial de la Federación.

La exposición de motivos contiene interesantes proposiciones que justifican la creación de esta Ley, reconociendo que implica la salvaguarda de los derechos fundamentales, apoyando nuestra postura garantista:

> La protección de datos implica la salvaguardar los **derechos fundamentales**.
>
> La decisión de crear un ordenamiento jurídico es una consecuencia tardía pero necesaria sobre Protección de Datos.
>
> Es innegable la relación entre **la protección de datos y los derechos fundamentales** de las personas.

La protección de datos personales contenidos en bases de datos públicas o privadas es el objeto de esta legislación:

> La iniciativa que se pone a consideración del Pleno tiene por objeto **garantizar la protección de los datos personales que se encuentren contenidos en documentos, archivos, registros, bancos de datos, o bien, en otros medios tecnológicos de procesamiento de datos, sean de carácter públicos o privados**, a efecto de proteger los derechos de las personas a la vida privada y a la intimidad, así como el acceso a la información que sobre las mismas se registre, en términos de los artículos 6, 14 y 16 de la Norma Suprema.

Las disposiciones generales de esta ley establecen que será aplicable a las personas jurídicas, haciendo énfasis que no se podrán afectar los registros y fuentes periodísticas, amen de que los archivos, registros, bases o bancos de datos electorales etcétera se regirán conforme a los ordenamientos aplicables y las excepciones de la presente ley.

Se señalan las definiciones precisando que se debe entender por base de datos Instituto y datos íntimos entre varios conceptos:

> Artículo 4.- Para los efectos de la presente ley se entenderá por:
>
> I. Base de datos: es el conjunto organizado de información que constituye datos personales que son objeto de tratamiento o procesamiento, por medios electrónicos o manuales, entre otros, sin importar la modalidad de su formación, almacenamiento, organización o acceso.
>
> II. Instituto: Al Instituto Federal de Protección de Datos Personales;
>
> III Datos íntimos: Datos personales relacionados con las características físicas, morales, psicológicas o emocionales de la persona, con su vida afectiva y familiar, con su origen racial o étnico, con sus preferencias sexuales, así como con sus convicciones religiosas, opiniones ya sean políticas o, de otra índole, con sus estados de salud física y emocional.

> **IV.** Datos personales: Información referente a una persona física, determinada o determinable.
>
> **IX.** Tratamiento de datos: las operaciones y procedimientos sistemáticos, físicos o electrónicos, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, reproducción, transmisión y destrucción, entre otros, de datos personales.
>
> **X.** Usuario de datos: Persona de carácter público o privado que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

Dentro de estas definiciones la de datos personales no es muy atinada y es preferible aceptar la que señala la LFTYAIPG, los datos "íntimos", serían más correctos al ser denominados sensibles, como la doctrina los ha conocido, aporta conceptos interesantes como el de tratamiento de datos y usuario de datos incluyendo a personas de carácter público o privado.

El capítulo tercero señala que queda prohibido el tratamiento, que comprende desde la recolección hasta su divulgación, de datos personales que revelen ideologías, origen racial o étnico, convicciones religiosas y no religiosas o de cualquier tipo, hábitos y comportamientos personales, orientación y vida sexual, rasgos físicos y psíquicos, estado de salud, opiniones políticas, afiliación partidaria, salvo que los ordenamientos jurídicos dispongan lo contrario o medie consentimiento de su titular siempre que no sea factible su identificación:

> Artículo 5.- Queda prohibido el tratamiento de los datos personales que revelen ideologías, origen racial o étnico, convicciones religiosas y no religiosas o de cualquier tipo, hábitos y comportamientos personales, orientación y vida sexual, rasgos físicos y psíquicos, estado de salud, opiniones políticas, afiliación partidaria, salvo que los ordenamientos jurídicos dispongan lo contrario o medie consentimiento de su titular siempre que no sea factible su identificación.

Existe una excepción a la transferencia de datos que resulta amplia y que en la actualidad ha generado mucha polémica, ya que en aras de la cooperación internacional y la lucha contra el terrorismo, se ceden datos personales que finalmente no sabemos donde terminarán, si en los archivos de la CIA o en las bases de datos del departamento de marketing de *Procter & Gamble,* veamos:

> **Artículo 24.- No se podrá realizar la transferencia de datos personales** de cualquier tipo con organismos, autoridades o entes públicos o privados del extranjero, así como organismos internacionales, cuando no proporcionen niveles de protección adecuados, **salvo en los siguientes casos**:
>
> I. Colaboración judicial internacional;
>
> II. Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o bien se trate de una investigación epidemiológica, siempre que se hubiera utilizado un procedimiento de disociación de información;
>
> III. Cuando la transferencia se hubiera acordado en el marco de tratados internacionales suscritos por los Estados Unidos Mexicanos;

> IV. Cuando a transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, los delitos contra la salud, las operaciones con recursos de procedencia ilícita, **el terrorismo y el financiamiento al terrorismo**.

En este proyecto de Ley toda persona puede solicitar información al organismo de control relativo a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables, así la consulta pública y gratuita.

El control estará a cargo del Instituto encargado de controlar, organizar, estructurar, evaluar y vigilar la protección de los datos personales, que se encuentran en los bancos de datos, archivos o registros; así como a los responsables de los mismos, regulados por esta ley, será el que disponga la Ley Federal de Transparencia y Acceso a la Información Pública. El cual será un órgano dentro del IFAI que será integrado por tres comisionados (del artículo 52 al 55 del Proyecto de Ley). Se contienen también sanciones donde el Instituto podrá apercibir a los usuarios cuando incumplan sus obligaciones.

La acción de protección de los datos personales instituye que los titulares de los datos personales podrán ejercerla, para conocer los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, así como la finalidad de aquellos y para solicitar la rectificación, supresión, confidencialidad o actualización de los datos personales en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro este prohibido. La acción es de carácter jurisdiccional ya que será el juez del domicilio del actor el que conocerá de dicho recurso legal, pero no nos queda claro que tipo de juez se trata, se infiere que es un juez local en materia civil pero a la vez se contempla la posibilidad de que sea un juez federal, existe opacidad en cuanto a la forma de determinar la competencia y jurisdicción de esta acción:

> **Artículo 60.-** Será competente para conocer de esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor.
>
> Procederá la competencia federal cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones, nacionales o internacionales.

Se establece un procedimiento con plazos y términos que no es muy claro, por lo que resulta de difícil comprensión a toda la sociedad, debiera ser un procedimiento sencillo como se ha planteado la solicitud de información y el recurso de revisión en la Ley Federal de Transparencia.

Es interesante repasar lo sucedido en la sesión del jueves 2 de febrero de 2006 en la que el Senador García Torres presentó un proyecto de decreto de una Ley Federal de Protección de Datos Personales distinta a la aquí comentada,

previniendo: "Los documentos de trabajo que fueron elaborados en estas reuniones fueron puestos a consideración de las comisiones dictaminadoras, especialmente de la Comisión de Gobernación de la Cámara de Diputados sin que se tomara estos documentos y todas las reuniones en cuenta. Desconociendo todo esto, el diputado Jesús Martínez Álvarez presentó una iniciativa de Ley Federal de Protección de Datos Personales en la sesión de 1 de diciembre de 2005, ante el Pleno de la Cámara de Diputados, el cual no es más que un *mutatis mutandis*, una copia de la Ley Federal de Protección de Datos Personales presentada por el suscrito."[353] Esta declaración denota una total descoordinación entre ambas Cámaras Legislativas, muestra del desorden y desaseo en la función creadora de leyes o tal vez un artilugio político para no dar paso al proyecto García Torres.

2.- Iniciativa de Ley Federal de Protección de Datos Personales, presentada por el Senador Antonio García Torres, Partido Revolucionario Institucional, el 2 de febrero de 2006.

Esta iniciativa parece ser la más seria, discutida e importante de las que se han presentado. Tiene su antecedente en una propuesta presentada el 14 de febrero de 2001, por el mismo legislador, que tuvo una trayectoria larga y tortuosa que culminó con un dictamen no aprobatorio. El día 30 de abril de 2002 el proyecto fue aprobado y publicado en la Gaceta del Senado; mientras que la Ley de Transparencia y Acceso a la Información Pública Gubernamental ya había sido aprobada y se había ordenado su publicación en el Diario Oficial de la Federación quedando pendiente la de Ley de Datos Personales en la Cámara de Diputados. Esto a razón de un acuerdo parlamentario[354] de votar ambas leyes.

Asesores de la Cámara de Senadores trabajaron de forma coordinada con servidores de la Cámara de Diputados con el fin de impulsar la iniciativa e, incluso, con el ánimo de que México contara con una regulación en la materia de protección de datos. También existió un contacto constante y abierto con sectores públicos como Banco de México, Secretaría de Gobernación, IFAI, y con organismos privados como la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información, sociedades de seguros, representantes de tarjetas de crédito y otros interesados.

Nos narra García Torres lo que aconteció:

> "Posteriormente, el día 14 de diciembre de 2005, sin que estuviera listada en la orden del día correspondiente y ya comenzada la sesión plenaria de la Cámara de Diputados del Congreso de la Unión, se solicitó que se incluyera como un asunto a discutir el dictamen en sentido negativo de la ley presentada

---

[353] ***Versión estenográfica de la Sesión Pública Ordinaria de la Cámara de Senadores celebrada el jueves 2 de febrero de 2006***, Servicios Legislativos de la Cámara de Senadores, México, D.F. disponible en línea: http://www.senado.gob.mx/servicios_parlamentarios.php?ver=estenografia&tipo=O&a=2006&m=02&d=02

[354] ***Acuerdo parlamentario***.- Resolución que se toma al interior de los órganos de gobierno del Congreso – que se somete a la aprobación del pleno-, para establecer normas o lineamientos donde la legislación es limitada. QUINTANA VALTIERRA, Jesús y CARREÑO GARCÍA, Franco, ***Derecho Parlamentario y Técnica Legislativa en México***, Editorial Porrúa, México, 2006, pág. 425.

por el suscrito, lo cual fue aprobado en votación económica y se acordó discutir en lo general y en lo particular en un solo acto, para que después el dictamen en sentido negativo fuera votado en forma económica por mayoría de legisladores.

Este proceder no solo es contrario a la práctica parlamentaria, sino también a lo previsto en la propia normativa que rige las actividades del Congreso, pues el dictamen debió de ser distribuido y publicado en la Gaceta Parlamentaria de aquella Cámara para ser discutido e inclusive en las votaciones del dictamen debieron ser nominales y no económicas como lo hicieron, violando lo dispuesto en los artículos 20, 36 de la Ley Orgánica del Congreso General de los Estados Unidos y el 117, 146, 147 y 148 del Reglamento para el Gobierno Interior del Congreso General.

En el dictamen negativo que solo fue publicado electrónicamente varios días después, se precisan como razones para no aprobar la minuta que contenía el proyecto de Ley Federal de Protección de Datos Personales argumentos sin fundamento."

Como podemos apreciar de las palabras del legislador existieron varias violaciones al proceso legislativo que dan a entender la no existencia de acuerdo por parte de la revisora, en base a opiniones de la industria y otros sectores. El Dictamen en sentido negativo, de la Minuta con Proyecto de Decreto por el que se expide la Ley Federal de Protección de Datos Personales,[355] contiene 16 puntos considerativos, por los cuales desecha el Proyecto del Senador García Torres. De los cuales tomaremos los que a nuestro parecer fueron los más importantes:

2. **Que esta materia, al no estar expresamente señalada en la Constitución la facultad del Congreso de la Unión para legislar al respecto**, se entiende una facultad concurrente entre la Federación, los Estados y los Municipios;
3. Que por otra parte, **las sociedades mercantiles en cualquiera que sea su giro, están reguladas por las leyes federales**. Las empresas de manera habitual realizan sus actividades a nivel nacional o regional sin reparar en las peculiaridades de las legislaciones locales;
4. Que de ser así, **el proyecto debiera contener lineamientos generales de las facultades que a cada orden de gobierno corresponden**, desarrollando el contenido de una ley general. Aún así, el proyecto propone expedir una ley de orden federal;
6. Que **el proyecto basado en la Ley española de 1992 no toma en cuenta los avances de las legislaciones expedidas con posterioridad**. El texto que se propone en la Minuta objeto del presente análisis **no recoge la mejor práctica internacional y los principios generalmente aceptados en la materia, tales como los elaborados por la Unión Europea y la Organización para la Cooperación y el Desarrollo Económicos (OCDE)**. El Derecho comparado demuestra que el modelo que se propone ya ha sido superado en la experiencia de otros países;
8. Que **el diseño institucional de la Ley es impreciso pues si bien establece como autoridad al recientemente creado Instituto Federal de Acceso a la Información Pública, no detalla las facultades necesarias para que este instituto pueda regular, controlar y supervisar la protección de datos personales**. Esta situación menoscabaría gravemente la capacidad del Instituto de regular la materia;

---

[355] ***Dictamen en sentido negativo, de la Minuta con Proyecto de Decreto por el que se expide la Ley Federal de Protección de Datos Personales***, Agencia Española de Protección de Datos Personales, diciembre 14 de 2005, https://www.agpd.es/upload/Canal_Documentacion/legislacion/Dictamen%20retirada%20Ley%20Mexicana.pdf

13. Que **la propuesta generaría un elevado costo para la economía, en particular para las empresas y entidades públicas con requerimientos de información**. Su efecto principal sería el detener el flujo de datos personales, afectando innecesariamente importantes actividades económicas;
14. Que la propuesta **busca fundamentalmente proteger la privacidad de las personas, sin embargo olvida las muchas y variadas razones por las que éstas pueden beneficiarse de compartir información personal**. Por ello, el proyecto no logra conseguir un equilibrio adecuado entre la protección de la privacidad y el flujo de información;
15. Que consideramos que este proyecto, de aprobarse, no lograría su objetivo de proteger los datos personales e **incluso podría producir efectos contraproducentes –tales como la migración de bases de datos- que pondrían en riesgo este objetivo; tendría altos costos e inhibiría seriamente la creación de los mercados de información, instrumentos determinantes en la competitividad y la eficiencia de la economía nacional**;
16. Que si bien es cierto que nuestro país debe contar con un instrumento legal que permita la protección de los datos personales presentes en el ámbito privado, esta Comisión dictaminadora sostiene que, la legislación que para este efecto se expida, **debe ser diseñada tomando en cuenta las particularidades de nuestro Sistema Jurídico y de las características de la actividad regulada, así como buscar que la normatividad recoja lo mejor de las experiencias internacionales**, en términos del Derecho Internacional Comparado.

Al respecto García Torres manifestó: "En el fondo, lo que muestra lo anterior, es que no existió una voluntad de legislar en la materia, cualesquiera que fueran las razones y que esto se hizo de manera conciente, deliberada, poco clara y sin argumentación jurídica. Esto se refuerza si se considera que el IFAI sostuvo opiniones próximas al rechazo de la iniciativa que echaron por tierra su posición anterior de apoyo a la regulación de datos personales, como quedó patente en el IV Encuentro Iberoamericano de Protección de Datos Personales, que fueron retomados en el propio texto del dictamen en sentido negativo, incluso casi en un sentido literal."

Esta iniciativa bien pudo haber sido modificada en los puntos que existía discrepancia, no hubo voluntad política para llevarla a buen término y en cambio se notaron intereses extraños por parte del IFAI y otros actores en la materia como lo es la industria.

Cabe señalar que las principales preocupaciones que tenía la industria según nos relata Reyes Krafft, consistía en primer lugar en mantener el *opt in* como forma de obtener los datos personales de los sujetos:

Artículo 8.
1. **La colecta y el tratamiento automatizado de los datos requieren del consentimiento previo del interesado**, salvo que la ley disponga otra cosa.

2. El interesado, sin su responsabilidad, tiene el derecho de revocar su consentimiento para el tratamiento automatizado de datos, dando aviso oportuno e indubitable al titular del archivo, registro, base o banco de datos, salvo que la ley disponga otra cosa.

> 3. **No se requiere el consentimiento del interesado, cuando los datos de carácter personal se colecten de fuentes de información de acceso público**, cuando se recojan para el ejercicio de las funciones propias de entidades y organismos públicos en el ámbito de su competencia, ni cuando se refieran a personas vinculadas por una relación comercial, laboral, administrativa, contractual y sean necesarios para el mantenimiento de la relación o para el cumplimiento del contrato.[356]

En segundo lugar se prohibía el flujo transfronterizo de datos personales ya sea a otros Estados nacionales u organismos internacionales que no proporcionen los mismos niveles de seguridad y protección que México:

> **Artículo 14.**
> 1. **Se prohíbe la transferencia de datos personales con Estados u organismos internacionales, que no proporcionen niveles de seguridad y protección cuando menos equivalentes a los que se proporcionan en el Estado Mexicano.**

Por último establece facultades discrecionales a la autoridad, con el fin de definir la tecnología a emplearse con el manejo de archivos:

> **Artículo 11.**
>
> 3. El reglamento de esta ley **determinará los requisitos y condiciones mínimas de seguridad y de organización, en función del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos**.

Estas son las más importantes oposiciones de la industria a la iniciativa de 14 de febrero de 2002.

Por otra parte, después de todo lo narrado se presentó una nueva iniciativa, la que fue presentada por el mismo García Torres el 2 de febrero de 2006, esta iniciativa sigue el modelo europeo, recoge algunas de las posturas que exteriorizo la industria como lo es el flujo transfronterizo de datos, pero mantiene el *opt in* que obliga a las empresas a obtener el consentimiento previo y expreso de los individuos para poder enviarles información, también contiene el registro de bases de datos ante el Instituto Federal de Protección de Datos Personales, manteniendo la creación de este organismo para la protección de datos.

En su exposición de motivos existen interesantes argumentos que refutan lo dicho en el Dictamen negativo, de los cuales únicamente utilizaremos los más importantes:

> Estos argumentos, en su mayoría son falaces (refiriéndose al Dictamen negativo) (argumento falaz es aquel que no se formula de manera correcta y

---

[356] Gaceta Parlamentaria año IV, No. 688 de jueves 15 de febrero de 2002, Cámara de Diputados, México, D.F. 2002 ***Iniciativa de Ley Federal de Protección de Datos Personales, presentada por el Senador Antonio García Torres del Grupo Parlamentario del Partido Revolucionario Institucional, en la Sesión de la Comisión Permanente del Miércoles 14 de febrero de 2002,*** http://gaceta.diputados.gob.mx/Gaceta/58/2001/feb/20010215.html#Ini20010215AntonioGarcia

que, sin embargo, de inicio parecería o se presenta como correcto o verdadero):

Los argumentos previstos en **los puntos 2 y 6,** relativos a que no se hicieron ajustes para adecuar la propuesta a la LFAIPG, tiene su origen en que la LFPDP fue presentada antes que el proyecto de la LFAIPG y en que fueron dictaminadas de manera conjunta en la Cámara de Senadores y porque se acordó que no se creara otro instituto diverso al IFAI y que no se modificaran más ambas propuestas.

Por otra parte, **es una falacia que la Constitución no otorgue facultades al Congreso de la Unión para legislar en la materia de datos personales, y tan es un argumento falaz que en la misma LFAIPG existen diversas disposiciones sobre protección de datos personales,** como existen en otras, baste citar a modo de ejemplo la Ley Federal de Protección al Consumidor (véanse los artículos 17, 18 y 19 de la Ley).

La competencia del Congreso de la Unión para legislar en la materia debe encontrarse en el mismo artículo 73, fracción XXX, en relación con las demás fracciones del propio artículo, y concordado con los artículos de la Constitución que otorgan competencias para legislar al Congreso de la Unión, vinculadas siempre al artículo 124.

Se dice que el proyecto de Ley Federal de Protección de Datos Personales no tomó en consideración "los avances de las legislaciones expedidas con posterioridad -a la Ley Orgánica de Regulación del Tratamiento de los Datos de Carácter Personal, *española* de 1992- -y que- no recoge la mejor práctica internacional y los principios generalmente aceptados en la materia", lo cual resulta incorrecto, primero al afirmar que el proyecto se basó en la LORTAD *española* de 1992 y luego al decir, implícitamente, que no se recurrió a una comparación más profunda, pues **bastaría decir que el proyecto de LFPDP rechazado tomó en consideración diversos instrumentos internacionales, que se reflejan en los principios que transpuso, por ejemplo, y que, contrario a la LORTAD, acogió experiencias latinas como la acción protectora de datos personales o *habeas data*, o bien que, fruto de un estudio comparado, había recogido de la legislación *italiana* la postura de reconocer que las personas morales tienen derecho a la protección de los datos personales, sino en los mismos términos que las personas físicas, sí en un sentido diverso.**

El dictamen, en este sentido, fundamentalmente confiesa un desconocimiento sobre el tema.

En cuanto a que no se hace un estudio sobre los impactos económicos de la Ley, cabe pensar que ello no es certero, pues **el fundamento económico de la iniciativa se encuentra en la idea base de que una regulación que garantice a las personas la seguridad en el tratamiento de los datos personales, generará confianza, precisamente en ese tratamiento, y que gracias a ello, las inversiones económicas se verían incentivadas,** siendo esta la postura de los diversos instrumentos internacionales en la materia.

Esta nueva iniciativa cambia en algunas cuestiones pero no es un cambio de fondo, simplemente adecua algunas de los argumentos esgrimidos y en otros no ofrece mayor solución. La cuestión del *opt in* puede traer como consecuencia mayor costo y dificultad de implementación a las empresas, la regulación de las bases de datos trae como problemas un control efectivo de las mismas y el asegurar que estén protegidas, la creación de un registro de los

responsables de las bases de datos lleva como consecuencia un costo de cumplimiento para la industria y un proceso burocrático que afecta al erario federal, por otra parte la imposición de medidas técnicas de seguridad no asegura la neutralidad tecnológica; la creación de otro organismo público implica mayor gasto al erario.

Un argumento más es el que hemos estudiado en el sentido que esta Iniciativa esta basada en el modelo europeo y que a la fecha no es compatible con nuestros principales socios comerciales, que tienen un sistema mixto de regulación.

Por lo tanto una legislación en la materia debe tener un sano equilibrio entre el derecho de protección a la vida privada y las obligaciones que tiene el Estado, como lo es la orden judicial, el lavado de dinero entre otros y las demás disposiciones relacionadas con las organizaciones que requieren recopilar, almacenar, procesar y tener en su poder datos personales, que muchas veces son necesarios para la operación de instituciones y empresas que deben contar con esa información.

3.- Iniciativa de Ley Federal de Protección de Datos Personales, presentada por el Diputado David Hernández del Partido Revolucionario Institucional, el 23 de febrero de 2006.

Esta iniciativa en lo general pretende regular las conductas de terceros en relación con los datos personales de los individuos, permitiendo a éstos, el derecho de decidir como proveer y controlar el acceso y uso de su información personal, deja en los particulares la responsabilidad del tratamiento de datos personales, mismos quienes atenderán en primera instancia la solicitud de tramite de rectificación, actualización o cancelación de sus datos y en segunda instancia será el Instituto.

En lo particular está conformada por La presente iniciativa de ley consta de 42 artículos, divididos en dos Títulos; el Primero con seis capítulos y el segundo también con seis. El primer Título se refiere a los Datos Personales y el segundo de la Protección de los Datos Personales.

En el Título Primero de los Datos Personales, Capítulo Primero, aborda las Disposiciones Generales, en el que se definen los principales conceptos, se establece que es de orden público, se define quiénes son los sujetos regulados y la definición de lo que debe entenderse como datos personales. Importante señalar que regula a personas físicas y morales y excluye de la aplicación de la ley a todos los organismos regulados por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. El concepto de datos personales que proporciona, es mucho más amplio y también contiene el inherente a los datos sensibles:

> **Artículo 4.**- Para efectos de la Ley se entenderá por:
> I. **Datos Personales:** La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o

que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio;

II. **Datos Sensibles:** La información de una persona concerniente a su , ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad; [357]

El Capítulo Segundo, se refiere en particular al tratamiento de los datos personales y se hace una referencia puntual al aviso de privacidad, eje toral de esta propuesta, definido en los artículos 7 y 8 del Proyecto, en donde establece la responsabilidad de quien trata los datos y limita su utilización al fin para el cual fueron recabados, incorporando los conceptos de fin primario y secundario, pilares en el tratamiento de bases de datos.

Artículo 7.- Cuando sea necesario proporcionar un aviso de privacidad, en términos del artículo anterior, éste deberá contener, al menos, la siguiente información:
I. La identidad del responsable que recolecta y/o trata los datos personales;

II. El fin primario y cualquier fin secundario para el cual se recolectan y tratan los datos personales;

III. El fin primario y cualquier fin secundario para el cual los datos personales deban o puedan ser divulgados;

IV. Las opciones y medios que el responsable ofrezca a los titulares para tener acceso a sus datos, corregirlos, modificarlos o cancelarlos, de conformidad con lo dispuesto en esta ley;

V. El responsable establezca para limitar el uso y divulgación de datos personales para fines secundarios, de conformidad con lo dispuesto en esta ley, y

VI. El procedimiento y medio por el cual el responsable notificará a los titulares de cambios sustanciales al aviso de privacidad, de conformidad con lo previsto en esta ley.

Artículo 8.- El aviso de privacidad debe hacerse disponible por cualquiera de los siguientes medios:
I. Cuando el tratamiento de datos se haga por cualquier medio electrónico, óptico o de cualquier otra tecnología, el aviso de privacidad debe estar disponible o referenciado en el momento del primer contacto con el titular de los datos, de forma clara y fehaciente.

Tratándose del tratamiento de datos vía Internet, el sitio, página o pantalla en que se efectúa el primer contacto con el titular, puede remitir a un vínculo, liga o pantalla subsecuente en la que conste el aviso de privacidad.

Asimismo, el aviso de privacidad puede presentarse en forma resumida, indicando al menos los elementos previstos en el artículo 7, fracciones I, II, III y IV, siempre y cuando se presente en forma completa en el vínculo, liga o pantalla subsecuente a la que se remita en el sitio, página o pantalla original.

---

[357] Gaceta Parlamentaria, núm. 1953-I, jueves 23 de febrero de 2006, Cámara de Diputados, México D.F., ***Iniciativa de Ley Federal de Protección de Datos Personales, presentada por el Diputado David Hernández del Partido Revolucionario Institucional, el 23 de febrero de 2006,*** http://gaceta.diputados.gob.mx/

II. Cuando el tratamiento de datos se realice por cualquier otro medio distinto de los establecidos en el numeral anterior, el aviso de privacidad completo debe estar disponible en el momento del primer contacto con el titular.

Es de hacer notar que los otros proyectos presentados, pretendían establecer una regulación de protección de datos personales basada en el control de las bases de datos, por sí mismos. Sin embargo, esto resulta técnicamente imposible, en virtud del dinamismo de las propias bases de datos, esta iniciativa propone un sistema de protección de los datos personales contenidos en las bases de datos que gira en un autocontrol de las mismas. Por lo tanto, se establece que habrá obligación para todo aquel que maneje datos personales de hacer del conocimiento del titular de los mismos, un aviso de privacidad el cual le concede al gobernado el control de la divulgación de sus datos con lo que le otorga certidumbre. El Capítulo Tercero, aborda el consentimiento del titular para el uso y divulgación, tanto nacional como transfronterizo de sus datos personales, haciendo especial hincapié en que en todo caso, se requerirá del consentimiento previo, tratándose de datos sensibles. En el Capítulo Cuarto se establecen disposiciones especiales respecto del uso y divulgación de las bases de datos, considerando en todo momento respetar la voluntad del titular de los datos quien otorga su consentimiento con lo dispuesto en el aviso de privacidad. Por tanto lo dispuesto en éste, aplicará asimismo, al cesionario. En el Capítulo Quinto se establecen las excepciones a los referidos en el párrafo anterior, que permiten agilizar el tráfico mercantil, como pudieran ser los servicios tercerizados, los prestados a controladoras y filiales, los que derivan de fusiones y adquisiciones o sean requeridos por autoridades.

Artículo 16.- Las restricciones previstas en el artículo precedente, no aplicarán a los siguientes casos:

I. La divulgación a terceros que presten servicios al responsable en relación con el uso de datos personales para fines primarios, o cualesquiera fines secundarios consentidos por el titular, siempre y cuando:

a) El responsable tenga celebrado un contrato que obligue al tercero a no usar o divulgar información de los datos personales, en todo cuanto no sea estrictamente necesario para cumplir los fines para los cuales los datos personales fueron revelados por su titular, así como a asegurarse de mantener la confidencialidad de la información de acuerdo con las condiciones y términos establecidos en el aviso de privacidad y;

b) El responsable permanezca como la parte encargada de la integridad y protección de los datos personales que han sido transferidos a un tercero para su tratamiento, incluyendo cualesquiera terceros fuera de la jurisdicción o territorio de los Estados Unidos Mexicanos.

II. La divulgación efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad del mismo grupo de la responsable, que opere bajo los mismos procesos y políticas internas;

III. Uso y divulgación de datos personales que se adquieran mediante la fusión, escisión o adquisición de una empresa, siempre que se respeten los fines establecidos en el aviso de privacidad;

> IV. Uso y divulgación en aquellos casos en los que el responsable actúe para:
>
> a) Proteger o defender legítimamente sus bienes o derechos; y/o
>
> b) Prevenir un daño o peligro inminente a una o más personas.
>
> V. Uso y divulgación en casos de requerimientos de autoridad debidamente fundado y motivado.

En el Capítulo Sexto se establece la posibilidad al responsable de administrar la información que, previa notificación a los usuarios, incorporar un nuevo fin secundario o ampliar el que ya ha quedado descrito en el aviso de privacidad.

El Título Segundo, de la Protección de Datos Personales en su Capítulo Primero destaca la obligación de establecer y mantener medidas de seguridad administrativas, técnicas y físicas, que permitan proteger los datos personales. Detalla también la obligación de que el responsable de definir una persona o departamento encargados de recibir y dar trámite a solicitudes, registrarlas u agilizar el flujo de información con los titulares.

> Artículo 19.- Todo responsable que lleve a cabo el tratamiento de datos personales debe establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales por daño, pérdida, alteración o destrucción; o del uso, acceso o divulgación no autorizados.
>
> Dichas medidas deben ser congruentes con la naturaleza y grado de confidencialidad de los datos personales de que se trate, el riesgo potencial para el titular de su uso o transmisión indebida, el estado de la técnica, las posibilidades económicas del responsable y el costo de su implementación.

El Capítulo Segundo aborda de una manera clara y objetiva cuales son los derechos de los titulares, destacando entre ellos, el derecho de acceso, corrección y cancelación de datos. El Capítulo Tercero establece el procedimiento de acceso del titular ante el responsable. El Capítulo Cuarto indica que las funciones de vigilancia e interpretación de esta Ley estarán a cargo del Instituto Federal de Acceso a la Información Pública Gubernamental pero acotando que esta Ley no entrará en vigor en tanto no se realicen las reformas y adiciones a su Ley, que tengan como finalidad, darle facultades con respecto de datos personales, referidos en la presente ley, eliminando como se planteaba en la iniciativa del Senado, la creación de un nuevo Instituto. El Capítulo Quinto establece el procedimiento administrativo de protección de datos personales ante el Instituto. Por último, el Capítulo Sexto establece las sanciones a los responsables y terceros que no cumplan con lo dispuesto en la ley.

Esta iniciativa de ley contiene elementos de valor, por una parte el concepto del opt out, que significa que el usuario puede optar por salirse de una base de datos sin haberse solicitado su consentimiento, esto implica una fácil implementación a las empresas y es lo que actualmente se aplica en la mayoría de sitios que obtienen información, el hecho de que no existe un registro limita

los costos para que no se tengan que implementar su tramite e incorporación en registro público, las medidas técnicas son de acuerdo con lo sensible que sea la información, de esta forma se atiende la necesidad de confidencialidad de los datos y el tamaño de la empresa para costear dichas medidas, se designa al IFAI como autoridad competente, utilizando así la autoridad existente generando menos gasto al erario, es congruente con los principios internacionales ampliamente reconocidos y compartidos con nuestros principales socios comerciales, contiene reglas claras de acceso a la información de los particulares, asegurando el control del titular sobre el uso de sus datos.

A nuestro modo de ver, esta Iniciativa contiene mejores disposiciones para regular la protección de la vida privada en Internet, pero es una lastima que se haya presentado en el ocaso de la anterior legislatura. Fue turnada a la Comisión de Gobernación para su dictamen, no ha sido aprobada por ninguna de las cámaras y hasta este momento no se ha presentado el dictamen correspondiente.

4.- Iniciativa de Ley Federal de Protección de Datos Personales, presentada por la Diputada Sheyla Fabiola Aragón Cortés del Partido Acción Nacional, presentada el 22 de marzo de 2006.

La presente propone una regulación más estricta respecto de los datos sensitivos sobre los meros datos de identificación. Se prevé la distinción elemental entre fines primarios y fines secundarios del uso de la información. En su desarrollo, los usos secundarios están necesariamente más regulados y exigen una mayor acción por parte de los responsables de la información para su manejo, se concentra esta iniciativa en la regulación de conductas y no versa sobre el registro o regulación de bases de datos. Se basa en las premisas básicas de la OCDE Y APEC estableciendo la obligación de toda entidad de proporcionar un aviso de privacidad. Se reconoce a las personas por su prerrogativa de manifestar su voluntad contraria al uso subsiguiente que se haga de su información, dando cabida al *opt out*.

Por cuanto toca al contenido de la propuesta iniciativa, ésta se compone de tres títulos, que versan sobre los datos personales, su protección y las autoridades y sanciones, respectivamente. En cuanto al primer título, se compone a su vez de seis capítulos. El primer capítulo contiene una serie de disposiciones generales, que incluyen un artículo de definiciones, así como un apartado de campo de aplicación, expresado en forma negativa, en relación con los sujetos que no están obligados al cumplimiento de la misma, por estar regulados bajo otros ordenamientos o leyes especiales en sus materias, al igual que la anterior iniciativa estudiada. Una primera distinción importante en la naturaleza de los datos personales se expresa en el propuesto artículo 4, que establece una categoría genérica de datos personales, dividida en dos especies, que son los datos de identificación, y los datos sensitivos. Los primeros guardan referencia con la información que permite identificar a una persona, en tanto que los segundos versan sobre sus condiciones o preferencias específicas, más allá de su mera identificación. La iniciativa propone una regulación más estricta

respecto de los datos sensitivos sobre los meros datos de identificación, puesto que la violación de su confidencialidad puede naturalmente atraer sobre las personas, mayores efectos o daños, en su caso, que la de su sola identificación.

> **Artículo 4.** Para los efectos de esta ley, se entenderá por
> **I. Datos personales.** Los datos personales de identificación, y los datos personales sensitivos.
>
> **II. Datos personales de identificación.** La siguiente información concerniente a una persona física, o moral cuando resulte aplicable:
>
> **a)** Nombre completo, incluyendo el nombre propio y sus apellidos materno y paterno respectivamente, o cada uno de éstos por separado;
>
> **b)** Domicilio completo o, a falta de éste, del lugar del centro principal de sus negocios, o en ausencia de éstos, del lugar donde simplemente resida;
>
> **c)** Correo electrónico, aun cuando tuviere varios;
>
> **d)** Número o números de teléfono o facsímile;
>
> **e)** Claves o números de identificación de documentos oficiales, tales como de la cédula del Registro Federal de Contribuyentes, la cédula profesional, la credencial para votar, el pasaporte, la Clave Única del Registro de Población (CURP) o similares;
>
> **f)** Cualquier otra información que permita identificar a una persona; o
>
> **g)** Cualquier otra información acerca de una persona que es tratada por una entidad regulada por la presente ley, en relación con todo o parte de cualquiera de los datos mencionados en los incisos anteriores.
>
> **III. Datos personales sensitivos.** La siguiente información concerniente a una persona física, o moral cuando resulte aplicable:
>
> **a)** Cualquiera que especifica o permite acceder o conocer balances o saldos de cuentas o estados financieros del titular, o en general datos relativos al conocimiento de claves o números de identificación personal de cuentas o tarjetas bancarias, de inversión, títulos u otros instrumentos de crédito; y
>
> **b)** Cualquiera relacionada con la condición médica o de salud, de origen racial o étnico, creencias religiosas, opiniones políticas o preferencia sexual del titular.

En atención a los estándares internacionales y la necesidad de que los sujetos obligados por la ley hagan del conocimiento de los titulares cuya información personal compartan, los fines específicos para los cuales se recaba y usa la información, se prevé la distinción elemental entre fines primarios y fines secundarios de uso de la información. Los fines primarios, por definición, corresponden a los propósitos con una relación o derivación directa y necesaria entre el receptor de la información y el informante, en tanto que los fines secundarios, como su nombre indica, tiene relación con propósitos subsecuentes o diferentes de los fines primarios para los cuales se recaban o usan datos personales en un determinado contexto. En el desarrollo de la ley

propuesta, los usos secundarios están necesariamente más regulados y exigen, en términos generales, una mayor acción positiva por parte de los responsables de la información para su manejo.

Esto nos lleva a otro concepto básico de la iniciativa, de acuerdo con las recomendaciones internacionales, consistente en la persona que deba estimarse como responsable del manejo de datos personales. En la práctica común ordinaria, las empresas y personas del sector privado en general, recaban y utilizan datos personales para la realización de sus actividades, lo que no necesariamente realizan de forma directa, sino que en algunos y no pocos casos, desde la recolección hasta el procesamiento y manejo de datos personales lo lleva a cabo un tercero por su cuenta y orden. En estas condiciones, la ley confiere un determinado grado de responsabilidad no sólo a quien aprovecha la información, sino también a quien funge como operador directo de su obtención y tratamiento. El mismo apartado de definiciones, al incluir el concepto de sistema de datos personales, reconoce la imposibilidad de categorizar o regular directamente a las bases o bancos de datos, independientemente de su forma, dado su número incierto, así como su naturaleza cambiante y extraordinariamente dinámica con el uso de las tecnologías actuales y las venideras.

El concepto de sistema de datos personales es un concepto amplio, que hace referencia e incluye, pero no se limita, a las bases o bancos de datos en la forma en que otra disposición legal o reglamentaria pueda definir, sino que abarca cualquier expresión automatizada o no, de datos clasificados o susceptibles de clasificación que mantenga u opere una determinada persona.

El capítulo segundo propone una serie de disposiciones en materia de recolección. El eje principal del capítulo, conforme a las premisas básicas de la experiencia internacional y particularmente de OCDE y APEC, lo conforma la obligación de toda entidad, sea que lo haga directa o indirectamente, de proporcionar un aviso de privacidad, que viene a constituirse en la principal institución legal de garantía respecto de la privacidad de que gozará la información que un titular comparta. El aviso de privacidad, o "notice", en la terminología internacional, es independiente de la forma en que se manifieste, pero en todo caso debe permitir la identificación del sujeto obligado y los fines para los cuales se recaba o usa la información. En este punto, la iniciativa propuesta sugiere la inclusión de un aviso amplio, que puede precisarse más o menos según la experiencia de cada sujeto obligado.

Por otra parte, es de reconocerse que, ante la vigencia de las tecnologías actuales, la forma de recolección suele adoptar dos formas básicas: la que en esta iniciativa hemos denominado "en línea", haciendo referencia a un mecanismo de tiempo actual y vigente en que interactúa el receptor con el informante, generalmente a través de un mecanismo automatizado o el Internet, y lo que se ha denominado "fuera de línea", en los casos en que, por exclusión, no ocurre en un momento de tiempo real, sino diferido o diferente respecto de una y otra parte.

> **Artículo 8.** El aviso de privacidad debe ponerse a disposición de los titulares de los datos personales de la siguiente manera:
> **I.** En recolecciones en línea, efectuadas por cualquier medio electrónico, óptico o de cualquier otra tecnología, en tiempo real, el aviso de privacidad debe proporcionarse en el momento de la recolección, de forma clara y fehaciente.
>
> En su caso, tratándose de recolecciones vía Internet, el sitio, página o pantalla en que se efectúa la recolección, puede remitir a un vínculo, liga o pantalla subsecuente en la que conste el aviso de privacidad.
>
> Asimismo, el aviso de privacidad puede presentarse en forma resumida, indicando al menos los elementos previstos en el artículo 6, fracciones I, III, y IV, de la presente ley y en forma completa en el vínculo, liga o pantalla subsecuente a la que se remita en el sitio, página o pantalla original.
>
> **II.** En recolecciones fuera de línea, el aviso de privacidad debe ser proporcionado a solicitud del titular, en el momento de la recolección de los datos personales o con posterioridad, de conformidad con lo previsto en esta ley.

El capítulo tercero versa sobre el uso de la información. De forma trascendente, se propone especificar los casos en que el uso de la información se da como una consecuencia necesaria o derivada de una relación legítima. En todos los eventos, se reconoce a las personas con su prerrogativa de manifestar su voluntad contraria al uso subsecuente que se haga de su información, independientemente de la causa que hubiera dado origen a la recolección o uso originales. Este mecanismo de *"opt-out"*, es la piedra angular que permite la interacción ágil y con la menor restricción posible al comercio, al tiempo que reconoce y otorga la prerrogativa de protección, libertad y control de las personas sobre la información de la cual son titulares. Esta excepción no se otorga tratándose de datos sensitivos, pues por su propia naturaleza es menester que su uso o aprovechamiento lo conozca o consienta su titular de forma previa.

El capítulo cuarto contiene un par de disposiciones especiales, propuestas en relación con el uso o divulgación por parte de terceros. En términos generales, la premisa básica de la manera legítima de compartir datos se funda en que la forma de divulgación incluya las restricciones a las que hubiere quedado sujeta su recolección o uso originales, si las hubiera, de manera resumida, la iniciativa propone una regulación *"in rem"*, esto es, que una causa o característica relativa a la información se estima "adherida" a ella, y la lleva de manera inherente, independientemente de la entidad o responsable que la trate.

El capítulo quinto contiene disposiciones cruciales para el mantenimiento del comercio regulado. Existen casos en que, natural y jurídicamente, la divulgación de datos personales a terceros no puede tener la misma sanción a que si aquélla se efectuara en supuestos ilícitos. En otras palabras, hay determinados casos en que la ley debe, mediante la institución de la reputación legal, considerar que la divulgación a terceros se lleva a cabo de manera lícita y consentida, pues de otra forma se impedirían actos de comercio de curso lícito. Estos casos, que son nuevamente los que aseguran y preservan la integridad

del sistema del comercio interestatal, están referidos a las relaciones contractuales previas entre el receptor y el informante, así como a casos específicos de acciones corporativas que, por su naturaleza, implican el conocimiento de información para llevarse a cabo.

El capítulo sexto refiere a un evento mayor de cambio en el uso o divulgación de datos personales, diferente al que hubiere ocasionado su tratamiento original. En este caso, se prevé que como un mecanismo protectivo, los sujetos obligados estén requeridos a realizar acciones positivas para que, en su caso, los titulares interesados puedan manifestar su voluntad contraria a usos subsecuentes no conocidos en el momento del tratamiento original.

A continuación, el título segundo refleja mayormente lo que las recomendaciones internacionales refieren como salvaguardas de seguridad. Sujeto a que las disposiciones reglamentarias abunden en los aspectos técnicos que corresponda, la ley anota en primera instancia, la responsabilidad y obligación de los sujetos obligados, de mantener medidas que razonablemente aseguren la protección de la privacidad de los datos personales compartidos por sus respectivos titulares.

> **Artículo 18.** Toda entidad regulada que recolecte, almacene, use o divulgue datos personales debe establecer y mantener medidas de seguridad administrativas, técnicas y físicas suficientes y adecuadas para
>
> I. Proteger los datos personales de cualquier uso, acceso o divulgación no autorizados; y
>
> II. Asegurar que la información es correcta, actualizada y pertinente para los fines para los cuales fue recolectada.
>
> **Artículo 19.** El nivel de medidas de seguridad administrativas, técnicas y físicas que deben ser operadas por la entidad regulada, debe ser congruente con la naturaleza y grado de confidencialidad de los datos personales de que se trate, el riesgo potencial para el titular de su uso o transmisión indebidos y el costo de su implementación.

Un capítulo segundo del título a que aludimos enuncia ahora los derechos de acceso, según las legislaciones modelo en la materia. La premisa fundamental del apartado consisten en dotar a los titulares, efectivamente, de un medio de petición expreso en la ley, entre particulares como lo es éste, de que se le confirme si un sujeto obligado tiene o no información personal que concierna al solicitante y, en su caso, que efectúe las rectificaciones que procedan, de acuerdo con la manifestación de voluntad que al respecto se le formule. La creación de este procedimiento de orden administrativo, aunque referido a particulares, es ciertamente un elemento que podría pasar por novedoso en nuestro sistema jurídico, aunque presente ya en otros ámbitos, y explicado también por la naturaleza propia de situaciones existentes entre particulares, pero que involucran valores tan altos como el derecho a la privacidad de las personas o la preservación del comercio interestatal en la Federación, ambos conceptos, necesariamente, de requerida protección estatal.

> **Artículo 20.** Toda entidad regulada que recolecte datos personales debe informar a su respectivos titulares, a solicitud de éstos, los datos personales que sobre ellos obren en su poder a efecto de que tales titulares puedan solicitar por escrito la corrección, modificación o supresión de dicha información, si ésta fuera incompleta, inexacta o tratada para fines distintos a los previamente consentidos.

Finalmente, el título tercero contiene prevenciones sobre las facultades del Instituto para sancionar a las personas que actuaren en contravención de las disposiciones de la ley. En este contexto, se estima que una orden de remisión expresa a las disposiciones de la Ley Federal de Procedimiento Administrativo es conveniente para evitar la creación de un mecanismo *ad hoc* que podría convertir la ley propuesta en un ordenamiento adjetivo, en perjuicio de su naturaleza de orden primario respecto de las materias que regula. Como se ha mencionado, si bien puede opinarse que el Instituto Federal de Acceso a la Información Pública es por definición un organismo rector de relaciones entre el sector público y los particulares, y no de relaciones que se establecen entre particulares, existen consideraciones de carácter presupuestaria e incluso del derecho administrativo que bien permiten evaluar la conveniencia de que sea el propio IFAI, y no un nuevo instituto, quien tenga a su cargo la función de ejecución de las disposiciones propuestas en esta iniciativa.

> **Artículo 30.** El Instituto será la autoridad competente para aplicar la presente ley

Esta iniciativa fue turnada a la Comisión de Economía y esta en espera de dictamen y aprobación por ambas cámaras. A nuestro sentir esta iniciativa mejora la del Senado y complementa la anterior emitida por la cámara de diputados, resulta ilustrativo ver como este proceso de implementación de una Ley Federal de Protección de Datos Personales ha originado mejorías en cada una de las subsecuentes iniciativas presentadas, lo que es lamentable es que los proyectos se queden durante meses incluso años, en los escritorios de diputados y senadores sin recibir siquiera un dictamen, aunque sea en sentido negativo como la Iniciativa García Torres, que a final de cuentas fue muy favorable para originar una mejor producción de propuestas legislativas. A la fecha de hoy mayo de 2007, no existe ninguna noticia sobre una posible aprobación o un nuevo proyecto presentado en la actual legislatura, esperemos que en breve se de el final de esta discusión para tener una protección a la vida privada dentro de Internet.

5.- Conclusiones sobre la implementación de una Ley Federal de Protección de Datos Personales en México.

A todas luces podemos concluir que la legislación es necesaria para proteger la vida privada de las personas y además salvaguardar los datos personales para que no exista un uso indiscriminado de ellos.

Podemos decir que la industria no esa en contra de la creación de esta ley, pero considera que debe tener características propias, para evitar gastos y burocracia, debe regular los datos personales y no las bases de datos, esta

legislación debe adoptar el concepto de "aviso de privacidad" que define el uso que se le da a los datos y la forma en que se pueden corregir y acceder, el *opt-out* para los datos no sensibles y el *opt-in* para datos sensibles, medidas de seguridad para recolección y tratamiento de datos congruentes con la confidencialidad de los mismos y la flexibilidad en el uso de tecnología según las capacidades económicas de la empresa responsable y por ultimo la existencia de una autoridad de la materia encargada de vigilar e interpretar la ley.

En las propuestas ya analizadas se recogen en diversa manera los principios anteriormente enumerados y buscan tener ámbito de aplicación en el sector público y en el privado, en dos iniciativas se propone la circulación de ciertos datos sin necesidad de contar con el consentimiento de los titulares, lo que se denomina *opt-out*, respecto de la autoridad que regulara la materia, la iniciativa del Senado es la única que prevé la creación de un nuevo Instituto Federal de Protección de Datos Personales, las demás iniciativas le dan atribuciones al ya existente IFAI.

Como lo vimos en todo este apartado, a pesar de contar con disposiciones jurídicas en la materia, es un hecho que resulta indispensable reglamentar el tratamiento de datos personales en México, a través de una ley que regule todos los sectores, a efecto de proteger la privacidad de las personas y establecer claramente si la explotación de los datos como actividad económica está por encima de la vida privada, o por el contrario, si es posible conciliar ambas exigencias. Cualquier decisión regulatoria adoptada tendrá un impacto inmediato en el sector industrial, por lo tanto es importante encontrar el balance entre la vida privada y la comercialización.

IV.- Legislación en materia de protección de datos personales en materia local: el caso Colima

De un estudio por entidades federativas encontramos que la única que tiene legislada la materia de protección de datos personales es el Estado de Colima y no es de extrañarse, ya que es de destacarse el avance que se tiene en la entidad en materia de automatización de servicios a la comunidad y otra actividades gubernamentales. Como ejemplos, pueden mencionarse los sistemas relacionados con el Registro Civil y la asignación de la Clave Única de Registro de Población CURP, los sistemas relacionados con las actividades notariales y del Registro Público de la Propiedad, los sistemas relacionados con las licencias de manejo y el control de vehículos, entre otros.

Esto, además de representar ventajas importantes para la población y un grado de modernización importante en el Estado, genera mayores riesgos en el mal uso que se le pudiera dar a la información, por parte de alguna autoridad, por algún empleado o por terceras personas, lo cual de nueva cuenta presenta una justificación para el desarrollo de una legislación en esta materia. Por otro lado, el sector privado en la entidad también ha venido digitalizando sus actividades, lo cual está generando un número creciente de bases de datos con información

sobre personas, con lo que también en este sector pueden empezar a tener riesgos. Se destaca que este proyecto es muy similar o casi idéntico a la primera Iniciativa García Torres por lo que esta ley ha intentado mantener congruencia con dicho documento, respetando los diferentes ámbitos de competencia de cada uno de los órdenes federal y local. Fundamentalmente, es necesario cuidar que se mantenga un adecuado balance entre el derecho a la intimidad y el derecho de los ciudadanos para conocer acerca de la actuación del gobierno. La Ley de Protección de Datos Personales se sustenta en el inciso VI del artículo 1 de la Constitución Política del Estado Libre y Soberano de Colima[358], que establece:

> "Las autoridades del Estado velarán por la defensa de los derechos humanos e instituirán los medios adecuados para su salvaguarda."

De lo anterior, se concluye que la privacidad personal es uno de los derechos fundamentales que protege la Constitución del estado de Colima en la fracción VI del artículo 1°.

- La protección de los datos de carácter personal es uno de los elementos esenciales de la privacidad.
- Los avances tecnológicos han incrementado los riesgos de un uso inadecuado de los datos personales.
- Resulta cada vez más fácil integrar datos personales de varias fuentes, posibilitando con ello que se identifiquen características privadas de las personas.

El estado de Colima se encuentra en un proceso acelerado de modernización que requiere de un uso cada vez más intensivo de la información personal y que resulta necesario resguardar los derechos de los habitantes en este respecto. La legislación es un paso importante para una protección adecuada ante las nuevas condiciones de desarrollo del Estado, conforme a la cual se determina que la información de carácter personal es irrenunciable, intransferible e indelegable, por lo que ninguna autoridad deberá proporcionarla o hacerla pública. Dicha información, así como la garantía de tutela de privacidad de datos personales, se regulará en los términos de dicta la ley. Con 23 artículos distribuidos en Seis Capítulos la ley se ocupa de los siguientes temas:
Disposiciones Generales;
De los Datos de Carácter Personal;
De la creación y protección de los datos personales;
De los archivos;
De la comisión; y
De las infracciones y sanciones.

En un primer plano, se precisa que la Ley será aplicable dentro del Estado de Colima, a los datos de carácter personal que sean registrados por los sectores público y privado en cualquier soporte físico que permita su tratamiento, y el

---

[358] ***Constitución Política del Estado Libre y Soberano de Colima***, H. Congreso del Estado Libre y Soberano de Colima, publicada en el Periódico Oficial "El Estado de Colima", los días 20, 27 de octubre 3, 10, 17 y 24 de noviembre de 1917, http://www.congresocol.gob.mx/leyes/Constitucion%20Local.doc

propio texto jurídico señala como datos personales, aquéllos relativos que de manera directa o indirecta puedan conectarse con una persona específica. De aquí surge la diversidad que la Ley contempla en cuanto al tratamiento de los datos personales, estableciendo dos grandes vertientes, los que se manejan en el sector público y los que se utilizan por el sector privado: La Ley en comento, establece disposiciones comunes para el manejo de datos de carácter personal, las que deben ser observadas tanto por dependencias del sector público como por personas físicas y morales del sector privado.

Así, en su Artículo Cuarto[359] señala que para el manejo de datos de carácter personal, se seguirán los siguientes principios:

1. Los datos que se obtengan deben ser adecuados, pertinentes y no excesivos;
2. Deben usarse para los fines que motivaron su obtención;
3. Deben ser correctos y actualizados;
4. Deben obtenerse por medios lícitos;
5. Para obtenerlos se debe informar al interesado la existencia y fin del archivo, las consecuencias de su suministro o de no proporcionarlos, la identidad y dirección del responsable del archivo.
6. Para el tratamiento de datos personales debe obtenerse el consentimiento explícito e inequívoco del interesado;
7. No podrán proporcionarse datos personales a terceros.

El sector público es una instancia en la que se concentran datos personales. Es común que los encontremos en los padrones electorales, catastrales, de contribuyentes, de instituciones de salud y de seguridad social, de conductores de vehículos, escolares, de beneficiarios de programas oficiales, de propietarios de inmuebles y de vehículos, por citar algunas fuentes, en la misma Ley se precisan diversas disposiciones para el tratamiento que el sector público debe otorgar a sus archivos, y que tienden a proteger la utilización de los datos de carácter personal, estableciendo genéricamente lo siguiente:

- Sólo se crearán, modificarán o eliminarán archivos previa disposición del Titular del Poder Ejecutivo, de los Presidentes Municipales o de los titulares de los organismos públicos, en su caso, publicadas en el Periódico Oficial;
- La disposición a que se refiere el punto anterior, deberá incluir:
  a).- La finalidad del archivo y los usos a los que se destinará;
  b).- Las personas o grupos que serán incluidos;
  c):- La obligatoriedad o carácter voluntario del suministro de la información;
  d).- Las características del proceso de obtención y del archivo, así como los tipos de datos de carácter personal que serán incluidos;
  e).- Las cesiones y comunicaciones de datos previstas;

---

[359] ***Ley de Protección de Datos Personales del Estado de Colima***, H. Congreso del Estado Libre y Soberano de Colima, publicada en el Suplemento No. 1 del Periódico Oficial "El Estado de Colima" No. 27, el sábado 21 de junio del 2003. , http://www.congresocol.gob.mx/leyes/Constitucion%20Local.doc

f).- El organismo responsable del archivo y, en su caso, cómo se pueden ejercer los derechos de acceso, rectificación, cancelación y posición;
g).- Las medidas de seguridad aplicables y el nivel de protección exigible;
h).-En casos de supresión de archivos, las medidas que se adoptarán para su destrucción;
i).- Las reglas aplicables para posibles fusiones o correlación con otros archivos.

- También se regulan los casos en que los datos contenidos en archivos públicos podrán comunicarse, exclusivamente, a otras instancias de las administraciones públicas estatal y municipales u organismos públicos, pudiendo ser:
  a).- Cuando se trate de la misma competencia,
  b).- Cuando se hubiera previsto en la disposición de creación del archivo;
  c):- Cuando una instancia de la administración u organismo público los procese para otra;
  d).- Cuando exista una orden judicial; y
  e).- Cuando el objeto de su comunicación sea con fines históricos, estadísticos o científicos.
- La Ley previene los casos en los que las entidades públicas podrán integrar archivos sin contar para ello con el consentimiento de los interesados, señalándose los siguientes:
  a).- Los que integren el Gobierno del Estado, los gobiernos municipales y el Instituto Electoral del Estado, con nombres y apellidos, Clave única del Registro de Población, domicilio, sexo, lugar y fecha de nacimiento, que sean utilizados para comunicaciones respecto a las funciones que les competen; mantenimiento y operación de los registros públicos establecidos en la legislación, mantenimiento y operación del listado nominal para efectos electorales; padrones de contribuyentes y control de vehículos y conductores.
  b).- Los que se integren con fines policiales.
  c).- Los que se integren para efectos fiscales, siempre que la obtención del consentimiento obstaculice la actuación de la autoridad durante el cumplimiento de sus funciones de recaudación;
  d).- También se podrán integrar sin autorización previa datos cuando obtener la autorización para ello impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de la autoridad, cuando afecte a la seguridad nacional o del Estado, a la seguridad pública o a la persecución de delitos o infracciones administrativas.

El Sector privado, por su parte, acrecienta permanentemente el número de archivos que contienen datos personales, para su utilización directa o, en algunos casos, para comercializar los mismos, tenemos en este contexto a las instituciones de carácter crediticio, las cadenas de tiendas departamentales, de reparto de correspondencia o documentación en general, ventas a distancia, prospección comercial y actividades similares. Al respecto la Ley establece, para la creación de archivos que contengan datos de carácter personal, de parte del sector privado, que:

- Podrán crearse cuando sean necesarios para lograr los objetivos legítimos del titular;
- Deberá notificarse su creación, el nombre del responsable y su domicilio, a la Comisión Estatal para el Acceso a la Información Pública;
- En los casos de investigaciones sobre genealogía o estudios biográficos, cuando los interesados tengan menos de 100 años de haber fallecido, podrán crearse los archivos sin autorización de los familiares, pero se requerirá autorización previa de la Comisión para ceder los datos correspondientes. Si los interesados tuvieran más de 100 años de haber fallecido, su tratamiento se considerará histórico y no sujeto a la Ley de Protección de Datos Personales.

Genéricamente, la Ley concede al ciudadano, de manera expresa las siguientes acciones: Acceso; rectificación; oposición; y cancelación de datos.

Se establece que la Comisión Estatal para el Acceso a la Información Pública será el organismo responsable de la tutela de los derechos consignados en la propia Ley, concediéndole las siguientes facultades: Vigilar el cumplimiento de la ley; Emitir las autorizaciones e instrucciones previstas por la Ley; Atender las peticiones y reclamaciones de los afectados, evaluarlas con audiencia de los responsables de los archivos y dictar las medidas tendientes a adecuar el tratamiento de los datos a las disposiciones legales; Informar a los ciudadanos de sus derechos en la materia y prestarles asesoría; Expedir los reglamentos de la Ley; y Elaborar y mantener el registro de protección de datos.

A manera de conclusiones podemos mencionar, que solamente el Estado de Colima cuenta con legislación específica para proteger a las personas de un uso indebido de sus datos personales; en algunas otras entidades las leyes de acceso a la información pública contienen disposiciones aisladas en este tema que resultan insuficientes para su adecuada regulación. Por otra parte la aplicación de la Ley en Colima ha encontrado cierta complejidad, particularmente con motivo de que un alto número de archivos del sector privado que contienen datos personales de habitantes del Estado se concentran desde entidades ajenas, donde no es factible aplicar las disposiciones normativas en observancia del principio de territorialidad de la Ley. En consecuencia, es deseable que el resto de los Estados de la República cubran ese vacío legislativo o en su caso se homologuen principios federales de aplicación como se pretende hacer con la promulgación de la Ley Federal de Protección de Datos Personales y por último dada la complejidad existente para la aplicación de la Ley, particularmente en cuanto corresponde al sector privado, es conveniente dotar a los organismos que se instituyan para tener a su cargo esta tarea, de los recursos humanos, tecnológicos y financieros que hagan posible aplicarla en forma debida y exitosa. Por lo tanto esta legislación en el papel representa un avance importante pero en los hechos no ha marcado diferencia alguna o avances relevantes para proteger la vida privada de los ciudadanos de la entidad federativa.

CAPÍTULO CUARTO

INTERNET Y LOS NUEVOS MEDIOS DE COMUNICACIÓN ELECTRÓNICOS

CAPÍTULO CUARTO. INTERNET Y LOS MEDIOS ELECTRÓNICOS

I.- Introducción.

Hasta hace algunos años, nadie hubiera imaginado el desarrollo que ha alcanzado la industria de la computación. Inicialmente fue una tecnología muy complicada y de uso limitado para especialistas, pero en menos de 40 años ha logrado crecer de tal manera que se está volviendo indispensable hasta para desempeñar actividades cotidianas. Sin lugar a dudas, se ha convertido en el elemento central de la revolución industrial actual, ya que ha incrementado de manera inimaginable la productividad a un ritmo igualmente impresionante, constituyéndose en una valiosa herramienta para lograr gran aceleración en los diferentes campos del saber humano.

La simplificación en el tamaño y manejo de los equipos, el desarrollo de la comunicación más ágil y oportuna en todos los órdenes de la vida, ya sea económico, político, social o cultural, han sido algunos de los factores para que Internet haya cobrado gran importancia. La cultura tecnológica, redoblando esfuerzos y niveles de eficiencia, se incrementará en los próximos años, resultando la investigación y la dinámica en la comunicación el punto central del quehacer diario que permitirán la optimización de los recursos y promover la competitividad a nivel internacional.

El éxito de Internet es la libertad que ofrece. No existe ninguna compañía u organización que posea o controle Internet. No hay censura, no hay jefes, ni directores ni accionistas. No hay costos por largas distancias, ni costo por tiempo de acceso; el costo solamente depende de la integración de servicios que se desea obtener y su nivel de conexión, es decir, si el enlace es a través de una línea telefónica y un módem, o si se realiza un enlace de mayor envergadura. El costo dependerá del equipo que se utilice (estaciones de trabajo, equipo de súper cómputo, etc.) y del tipo de enlace necesario (satelital, fibra óptica, RDI, etc.). Cada organización, grupo o compañía que está conectado a Internet es responsable de sus propias máquinas y su sección de la línea. Entonces, ¿cómo es posible que exista y que se pueda obtener información de casi todos los puntos del planeta?

Para explicarlo un poco, antes de mostrar su historia y su evolución, se puede hacer una analogía con el idioma español. El idioma no es propiedad de nadie, y nadie cobra por usarlo. Como hispano parlante, es responsabilidad de la persona el aprender a usar el idioma con corrección y hacer lo que sea con él. La gente, con el uso cotidiano, lo transforma y modifica, evoluciona y genera nuevas palabras, giros y vocablos. De manera semejante ocurre con Internet. Pertenece a todos y a nadie.

Internet se ha convertido en un auténtico fenómeno social en México. Ha tardado bastante tiempo pero finalmente ha entrado desde las universidades, a

las empresas, a los centros educativos y a los hogares. El ordenador ha dejado de ser algo mágico para convertirse en un electrodoméstico más. Hoy en día ya se habla de la integración total entre la informática y la televisión. Las comunicaciones están cambiando día a día. Estamos presenciando el nacimiento de un nuevo mundo donde no existirán ni distancias ni fronteras

Este apartado nace con la intención de ser una breve introducción a Internet. Está pensado en función de lo que pretende el trabajo en general. No sería posible entender el medio por el que se obtienen datos personales sin saber siquiera como se utiliza y cuales son sus recursos, ofreciendo de una manera resumida información de lo que es la red, de los servicios que hay y de sus posibilidades. Desmitificando al ordenador y lo que lo envuelve, comprendiendo que el uso de la tecnología no está relacionado únicamente a las áreas técnicas del estudio, sino que la humanística también puede vincularlas, ya que al fin y al cabo son fenómenos creados por el hombre para el hombre.

II.- Internet: Red de redes.

1.-Concepto de Internet.

En primer lugar, es menester definir lo que es Internet, para lo cual utilizaremos los conceptos de distintas fuentes encontradas en la misma red, ya que existen numerosos manuales que nos explican como comenzar en el mundo de la Internet. A continuación pasaremos a las definiciones que consideramos más acertadas:

Según dicen algunos expertos,[360] "**Internet** es actualmente un preludio de lo que serán las autopistas de la información en un futuro no muy lejano. Internet es una red de redes, es decir, está formada por numerosas redes esparcidas por todo el mundo, y ofrece sus servicios a una gran cantidad (y creciente) de usuarios. "

Refiriéndose a un concepto más técnico de lo que es la red de redes, la Institución Española de Informática[361] nos da el siguiente concepto: "Internet es un conjunto de redes de ordenadores interconectadas que comparten el mismo protocolo de comunicaciones (TCP/IP). Su límite es el límite que tienen las redes que la integran. A parte de compartir el mismo protocolo de comunicaciones, el medio de conexión de estas redes son las líneas telefónicas."

---

[360]Concepto proporcionado por la Red de Estudiantes Españoles, en su ***Manual de Internet*** que puede ser consultado en la dirección electrónica: http://geminis.adi.uam.es/-pcobo/internet/manual/manual.htm

[361]Institución Española de Informática, en su ***Introducción al uso de Internet*** que puede ser consultada en: www.pass.es/ intro/e

La definición anterior es, quizás, la más exacta si queremos definir Internet. Todo aquello que se pueda añadir a ella, sólo serán datos estadísticos que servirán para entender un poco más la magnitud de Internet.

Para el Instituto Tecnológico Autónomo de México,[362] "Internet puede ser vista como una utilidad de información, cuyos beneficios se pueden subdividir en seis categorías principales:

- Puede intercambiar información de manera rápida y eficiente.
- Puede consultar expertos y gente experimentada en miles de campos.
- Puede recibir actualizaciones regulares en sus temas de interés.
- Puede tener acceso a su información desde muchas diversas locaciones.
- Puede traducir y transferir datos de diferentes tipos de computadoras.
- Puede utilizarla también para su entretenimiento y diversión. "

En un muy particular punto de vista podría conceptualizar a Internet como una colección de miles de redes de computadoras que proveen el medio para una comunicación eficaz con centros educativos y de investigación, así como los gobiernos de los Estados nacionales y entidades de negocios alrededor del mundo.

En la definición que me aventuro a desarrollar encontramos tres elementos fundamentales. Primero que se trata de una colección de miles de redes de computadoras, es decir que estamos hablando de una red de miles de redes interconectadas. Segundo nos proveen el medio para una comunicación eficaz, me refiero a que existe la conectividad y el intercambio entre ellas para poder crear una comunicación interactiva, dónde existan dos agentes, uno emisor y otro receptor. Tercero que esta comunicación se da entre los tres principales actores del desarrollo de la red: Centros educativos y de investigación, los gobiernos de los Estados nacionales y por último todas aquellas sociedades, asociaciones, corporaciones o individuos que se dediquen a celebrar negocios en todo el planeta.

2.- Concepto de red.

Hablamos de que Internet es un conjunto de redes conectadas entre sí, que es la red de redes, pero la duda que nos salta a la vista es ¿Que es una red de ordenadores?

---

[362] Página del Instituto Tecnológico Autónomo de México (ITAM), en su ***Introducción a Internet***, localizable en la dirección: http://www.itam.mx/hiper/internet.html

Desde un punto de vista muy superficial y sin entrar en detalles diremos que una red de computadoras es la interconexión de varias computadoras, donde cada uno de ellos puede interactuar con los demás, a través de un medio de transmisión, con el fin de intercambiar información y compartir recursos (impresoras, programas de aplicación, etc.). En adelante, nos referiremos a una red de computadoras simplemente como "red".

Podemos afirmar que red es un conjunto de ordenadores conectados entre sí. Dicha conexión se puede llevar a cabo de distintas maneras:

- Mediante cable que conecte los ordenadores entre sí.
- Utilizando la línea telefónica.
- Sistemas mixtos: cable y línea telefónica.

Para que la comunicación entre los ordenadores se lleve a cabo con éxito es necesaria la presencia de los siguientes elementos:

- **Servidores.-** Son los ordenadores dedicados a servir de interlocutor entre todos los usuarios. Tienen altas prestaciones tanto en la velocidad de procesamiento de datos como la capacidad de almacenamiento de estos.
  - **Cliente.-** Lo constituyen todas las computadoras personales o PC´s[363] conectados a la red. La importancia del rendimiento y capacidad de estos ordenadores no es tanta como la del servidor.
  - **Arquitectura propia.-** Se define como tal al conjunto de componentes que permiten la transmisión. En redes mediante cable son: tarjeta de red y cable de par trenzado. En redes vía telefónica: módem y línea telefónica.

Ya entendiendo como se compone una red de ordenadores podemos comprender lo que es Internet, pero aún no queda claro como está formada una red de redes, un ejemplo de una WAN o red principal (*Wide Area Network,* Red de área amplia) es la de nuestra máxima casa de estudios la UNAM.

Actualmente, la UNAM cuenta con una red principal o "*Backbone*" que provee el servicio de conexión a otras redes. *Backbone* o Espina Dorsal es un término utilizado para nombrar a aquella red que es el eje de conexión de otras redes. Podemos imaginar al *Backbone* como el tronco de un árbol cuyas ramas la conforman las distintas redes que pueden estar conectadas a esta red principal.

Si queremos comunicarnos con cualquiera de estos dispositivos lo podemos hacer de dos maneras: mediante una conexión individual o mediante una conexión directa (o conexión de red). Mediante estás conexiones a la red principal o *Backbone,* se puede acceder a Internet.

---

[363]El término PC, significa en su traducción al español, Computador Personal, en inglés quiere decir *Personal Computer.* Término que en su momento fue aclarado.

3.- Conexión a Internet

Para que un usuario pueda utilizar Internet es necesario que tenga una forma de acceso. A esta forma en conjunto se le conoce como cuenta en Internet y esta puede ser contratada con un Proveedor de Servicios de Internet (ISP según sus siglas en inglés, término que fue estudiado en el capítulo segundo), que a su vez tenga acceso al *Backbone* o red troncal, en el caso de nuestro país con la Red UNAM o con la Red Tecnológica Nacional. Las cuentas en Internet constan de las siguientes partes:

a) Clave de acceso (*login name*)

El *login name* es el nombre de acceso para el usuario dentro de Internet. Este constará de 2 a 8 caracteres y generalmente se utiliza la referencia que el usuario haya seleccionado por caracterizarlo en la Red. Este nombre debe ser único y con él, el usuario podrá acceder a Internet desde el sistema donde fue dado de alta.

b) Contraseña *(password)*

El *password* o contraseña es una clave que sirva para corroborar la identidad del usuario. Esta clave es personal y confidencial; solamente el usuario debe conocerla. El *password* puede constar de letras (en mayúsculas y minúsculas) y/o números. Un buen *password* debe tomar en cuenta lo siguiente:

- longitud de más de cinco caracteres y menor que ocho
- personal y secreto
- preferentemente una combinación de letras y números, evitando utilizar nombres propios o palabras comunes.
- cambiarlo periódicamente

c) Buzón Electrónico

Es el área destinada para almacenar los mensajes enviados por el correo electrónico hasta que los usuarios puedan tener acceso a ellos.

Es necesario señalar que tanto la clave de acceso como la contraseña y el buzón electrónico, son datos personales sensibles que deben ser protegidos no solo por el usuario, sino también por los PSI y en su caso por el Estado.

4.- Los Proveedores de Servicios Internet (*Internet Services Providers*)

Un centro servidor es una empresa que comercializa accesos a Internet. Facilitan a los usuarios los códigos que permiten el acceso a la red. Es

importante que el centro servidor esté situado cerca de nuestro domicilio (en la misma población).

Otro concepto[364] nos señala que un Proveedor de Servicios de Internet, es una organización comercial cuya principal finalidad consiste en proveer el servicio de conexión a Internet entre sus clientes sean personas físicas o morales.

Todas estas empresas tienen una forma de operar similar: se paga una cuota mensual que incluye, en modalidad de tarifa plana, un buzón de correo electrónico y acceso ilimitado a Internet. Algunos de ellos tienen una tarifa reducida que incluye buzón para correo electrónico y unas horas gratuitas de acceso a Internet, facturando el excedente a un precio que oscila alrededor de 20 pesos/hora. Muy pocos cobran cuota de entrada o conexión. Y lo más vigente y económico es la utilización de las redes de banda ancha que permiten el uso de la línea telefónica a la vez de estar conectado a Internet, las 24 horas del día por una tarifa mensual que no excede de los 400 pesos mensuales, entre los proveedores más exitosos en nuestro país, esta Prodigy que es de Telmex y Cableaccess, que es una filial de Cablevisión.[365]

A decir de Rojas Amandi:[366] "Los costos relacionados con la conexión al sistema Internet tienden a permanecer estables en los países industrializados desde hace algunso años. Sin embargo, debido a las fluctuaciones que sufre nuestra moneda, no es posible brindar un costo aproximado de lo que representaría el acceso en México", opinión que es muy razonable, aunque ya se ha logrado establecer parámetros equitativos e iguales en cuanto al costo de acceso así como formas alternativas de ingresar a la red sin contar con conexión y más aun sin ordenador, como son los *cyber* cafes.

Todos facilitan el *software* de conexión que acostumbra a ser *shareware* (en la red siempre podremos encontrar nuevas versiones para actualizarlo), para Marcelo Mejía, Alejandra Barrera y Federico Kulhmann, el *software*, programa o paquetería es un conjunto de instrucciones que causan que una computadora ejecute una función en particular.[367]

III.- Como funciona Internet.

Internet responde a una arquitectura *cliente-servidor*. Esto no quiere decir que sea una relación únicamente entre dos ordenadores. En el momento en que utilizamos alguno de los servicios que Internet ofrece se pone en funcionamiento un complicado entramado de aplicaciones y máquinas que hacen posible que ese funcionamiento sea correcto.

---

[364] BUENROSTRO, CUERVO, GUTIÉRREZ Y ROSADO, ***Los Negocios en Internet hoy y en México***, Mc Graw Hill, México, 1997. pág 13.

[365] Para consultar tarifas al día acceder a: www.prodigy.net.mx, o www.cableaccess.com.mx

[366] ROJAS AMANDI, Víctor Manuel, ***El uso de Internet en el derecho***, Oxford University Press, México, 1991, pág. 10.

[367] MEJIA, Marcelo, BARRERA, Alejandra y KULHMANN, Federico, ***Introducción a las tecnologías de la información y de las comunicaciones (TICS) y a su aplicación en los negocios electrónicos***, en NAVRRO ISLA, Jorge (coord), ***Tecnologías de la Información y de las comunicaciones: Aspectos legales***, Editorial Porrúa e ITAM, México, 2005, pág. 9.

Acceder a la red Internet y "*navegar*" por ella no supone otra cosa más que enviar y recibir información a los distintos ordenadores que hay conectados a la misma. Estos ordenadores con los que interactuamos cuando estamos en Internet se llaman servidores. Los servidores están constantemente en espera de peticiones. Cuando yo quiero acceder a una página *web,* lo que el ordenador hace es enviar un mensaje al servidor dónde está la página. El servidor recibe el mensaje, lo procesa, y me responde enviándome dicha página para que yo la pueda ver en mi ordenador. El software que se encarga de llevar a cabo toda esta tarea de solicitar la página y luego interpretarla se llama *browser* o navegador, que más adelante estudiaremos. Una página *web* no es más que un fichero de texto escrito en un formato concreto, de modo que a fin de cuentas, los servidores de Internet son servidores de archivos que están constantemente recibiendo peticiones de ficheros y atendiéndolas.

1.- Anfitriones: Host.

En Internet se llama *Host* a cualquier ordenador que esté conectado a la red y que dispone de un número **IP** y un nombre definido. De una manera más sencilla: un Host o anfitrión es cualquier ordenador capaz de recibir o enviar información a otro ordenador.

2.- Identificación de un host *en Internet.*

Para navegar por Internet, lo primero que se debe saber es: ¿Qué es una dirección?, ya que para acceder a los servicios dentro de la red siempre habrá que especificar al menos una.

Todas las máquinas conectadas a Internet tienen una dirección numérica única e irrepetible, llamada dirección IP y sirve para poder comunicar a unas máquinas con otras. La dirección no se asigna arbitrariamente, se debe hacer una petición al *Network Information Center (NIC),*[368] el cual es el organismo

---

[368] El Network Information Center - México, (www.nic.mx) es la organización encargada de la administración del nombre de dominio territorial (*country code Top Level Domain*) .MX, el código de dos letras asignado a cada país según el ISO 3166.
Entre sus funciones están el proveer los servicios de información y registro para .MX así como la asignación de direcciones de IP y el mantenimiento de las bases de datos respectivas a cada recurso.
Este nace el 1ro. de Febrero de 1989, cuando el ITESM, Campus Monterrey establece conexión directa a Internet. *Merit Network, Inc* indica Febrero de 1989 como la fecha de conexión de México a NFSNET (Internet). En esos momentos se conecta el primer equipo a Internet bajo el dominio .mx: dns.mty.itesm.mx con la dirección 131.178.1.1.
Esta máquina, una Microvax-II, digital, fue el primer servidor de nombres para el dominio .mx. Lo fue hasta el 6 de Septiembre de 1993 (fecha del 50 aniversario del sistema ITESM), la sustituyó una Sun SPARC Classic con 48 MB en RAM y 400 MB en disco. En ese entonces no se requirió de una administración dedicada, ya que no existían muchos nombres de dominio. Para 1992 había sólo 45 dominios bajo .mx, de los cuales 40 eran académicos y 5 eran comerciales. Incluso .mx fue plano, sin clasificaciones, hasta Octubre de 1993, cuando en una reunión de los principales actores de las redes en México, se acordó crear los subdominios COM.MX, GOB.MX, y es en esa misma junta (en la Universidad de Monterrey) donde se decide no crear el subdominio EDU.MX. A principios de 1995 eran poco más de 100 nombres de dominio ubicados bajo .mx. Y sería precisamente a solicitud de la misma universidad que se iniciara una discusión pública en línea para la creación del dominio .edu.mx, y como resultado del consenso en la discusión del tema, el 4 de septiembre de 1996 se crea el edu.mx el cual junto con .mx representaba a dominio educativos. A mediados de 1997 se limita el registro de dominios académicos al .edu.mx. Después del "boom" del WWW en México, se registró un incremento considerable en el número de dominios registrados mensualmente, lo que requirió una administración dedicada, así como la puesta en marcha de algunos servicios, tales como: Registro en línea de nombres de dominio, solicitud de las IP, registro de ISP en el país, solicitud de ASN; todo ello a través páginas de WEB.
En Octubre de 1995, se hace oficial la designación del ITESM, Campus Monterrey como NIC para México, lo que se formaliza el trabajo que se había venido desarrollando desde 1989. Por primera vez en 6 años del código territorial, hay

responsable de la administración de las direcciones de toda la red y utilizar las que se hayan asignado.

Cada ordenador en Internet tiene una dirección (*IP address*) única y exclusiva que lo distingue del resto de los ordenadores de la red. Esta dirección o número IP está formada por cuatro números separados por puntos, cada uno de los cuales puede tomar valores que oscilan entre 0 y 255. Las direcciones se componen de cuatro octetos (grupo de números) separados por puntos. Por ejemplo, la dirección 148.202.3.5 corresponde al servidor serpiente.dgsca.unam.mx de la Universidad Nacional Autónoma de México.

---

mas dominios comerciales que dominios educativos. A finales de año los dominios comerciales representaban el 55%. En Diciembre de 1995 se hace el anuncio de los servicios de NIC-México, para entonces se contaba con listas de correo y FTP anónimo. A finales de ese año había 326 nombres de dominio bajo .mx.

Durante 1996 se adquiere un nuevo equipo, una SUN SPARC 20, 256 MB RAM. Se empiezan a desarrollar servicios de registro automatizados y eficientes. A finales de este año había 2838 nombres de dominios bajo .mx y el 80% de ellos eran dominios comerciales. El crecimiento acelerado en el número de dominios hace necesario un mantenimiento de Bases de Datos actualizadas y en línea para la operación diaria del Internet en México, por lo que NIC-México evoluciona y en Enero de 1997 empieza a funcionar la Base de Datos WHOIS para el dominio .mx.

En este mismo año se realiza la 1ra. Reunión de Información y Retroalimentación de NIC-México en la que buscamos informar a nuestros clientes de los últimos acontecimientos en Internet y obtener retroalimentación de ellos respecto a nuestros servicios. Se fijan cuotas de cobro por registro y mantenimiento de los dominios. Los dominios de entidades gubernamentales sobrepasan los 100 y el total de dominios registrados hasta 1997 es de 7251.

Para 1998 estábamos en los 10,000 nombres de dominio registrados y pagados lo que permite adquirir una infraestructura más robusta y confiable: Un enlace de 128K con UNINET, uno de 256K con AVANTEL y 10MB con el ITESM, Campus Monterrey; servidores SUN 450, 250, Ultra 2 y Sparc 20 y equipo de ruteo cisco 7200 y 2500. En Marzo de este mismo año disminuimos las tarifas de registro y mantenimiento en 30%. A mediados de año realizamos la primera depuración de nombres que no tenían una resolución correcta o que tuvieran pagos pendientes. Durante 1998 surge la necesidad de asociarse con otros administradores de códigos territoriales (ccTLDs) para compartir información y discutir políticas de nombres de dominio. Es el 21 de Agosto de 1998 cuando NIC-México es co-fundador y representante interino de LACTLD, organización que agrupa a los dominios nacionales de Latinoamérica. Asimismo, NIC-México organiza en Monterrey la segunda reunión de DNSO, una de las organizaciones de soporte para ICANN, la corporación a cargo de la supervisión de los principales recursos de Internet.

En abril de 1999, con el nombre de dominio nestle.com.mx, se inicia la relación entre NIC-México y el Instituto Mexicano de la Propiedad Industrial (IMPI) para resolver disputas de nombre de dominio por cuestiones de propiedad intelectual.. Posteriormente se definieron mecanismos formales para resolver estos casos. Para mediados de este año son más de 20,000 los dominios registrados bajo .mx. En septiembre de 1999 entran en vigor nuevas políticas generales, las cuales contienen un procedimiento de resolución de disputas. Este procedimiento tuvo como objetivo resolver los casos más simples de disputas entre marcas registradas y nombres de dominio. De manera exitosa se resolvieron casi 60 casos en 15 meses.

En enero del 2000 había más de 30,000 dominios registrados. Para diciembre de este año hay nuevas políticas y un nuevo procedimiento de resolución de disputas, el cual ahora es administrado por la Organización Mundial de la propiedad Intelectual (OMPI), este procedimiento esta basado en el "*Uniform Dispute Resolution Policy*" (UDRP) el cual es el mismo mecanismo de resolución de disputas utilizados en los dominios genéricos en todo el mundo. OMPI reconoce a NIC-México por la implementación de esta política.

En enero del 2001, con más de 60,000 dominios registrados, se libera un nuevo sistema de operación, el cual además tiene una nueva imagen, con este sistema es posible llevar una mejor administración de los registros, modificaciones y pagos. Además una nueva Base de Datos que cumple con las recomendaciones hechas por la OMPI en relación al registro de dominios. Durante el verano del 2001 se establece el Comité Consultivo Externo de NIC-México con el objetivo de ser un órgano de consulta, orientado a discutir temas estratégicos y de política para emitir recomendaciones al NIC que coadyuven a alcanzar sus objetivos, con la intención de apoyar el fortalecimiento de NIC-México, así como de impulsar el desarrollo de Internet en México.

A finales del 2001 se realiza una fuerte inversión en infraestructura tecnológica como base para los proyectos de NIC-México en puerta, principalmente para migrar nuestros equipos de cómputo a uno de los centros de datos más avanzados en el mundo y el mejor en Latinoamérica.

Para el 2002 ya hay 75,000 dominios registrados en el .MX siendo el com.mx quien contiene casi el 93% de los registros.

A principios del 2003, con la recomendación positiva del Comité Consultivo, se publican nuevas políticas que entre otras cosas permiten que el nombre de dominio se registre inmediatamente sin intervención humana, se promueve la libertad del registrante de elegir el nombre de dominio que considere apropiado sin revisión de NIC México. Así mismo se redefine la política de solución de controversias, conocida como LDRP. En julio del 2003, NIC México robustece aún más su infraestructura tecnológica y se convierte en el primer ccTLD en desarrollar e implementar el esquema *Shared Unicast (Anycast)* en sus servidores secundarios, esquema utilizado en los *Root Servers*. ***NIC, México***, www.nic.mx

Pero para el usuario resultaría más cómodo que el identificador de las máquinas tuviese una forma más sencilla. Existe otra forma de identificar cada ordenador dentro de la red, más intuitiva y geográfica. Se trata del *nombre de dominio*. Si bien el número IP es la forma que tienen los ordenadores de llamarse entre sí, las personas suelen referirse a los ordenadores con el nombre de dominio. Los nombres están formados por conjunto de palabras separadas por puntos. Cada palabra representa un subdominio que está incluido a su vez en un dominio mayor. Se trata de una estructura jerárquica en la que los dominios se van escribiendo en orden de importancia.

Por ejemplo, para la máquina anterior su equivalente sería:

148.202.3.5 serpiente.dgsca.unam.mx

Donde:

serpiente es el nombre del servidor
dgsca es el grupo de máquinas que forman un dominio
unam dominio que hace referencia a la Universidad Nacional Autónoma de México
mx dominio que hace referencia a México

Y la siguiente dirección:

usuario@serpiente.dgsca.unam.mx

significa que usuario se encuentra en la máquina serpiente.dgsca.unam.mx. El símbolo @ significa: "en".

El sistema de nombres de dominio (DNS) es el sistema que se encarga de convertir una dirección numérica en nombre y viceversa.

Para el buen funcionamiento de las comunicaciones en la red, existen ordenadores (servidores de nombres) que se encargan de "traducir" de números a nombres (más fáciles de recordar).

3.- URL (*Universal Resource Locator*)

Cuando un usuario desea conectarse a un sitio en Internet a través de un navegador utiliza dirección de un servidor WWW. A esta dirección se le conoce como URL. Y éste se forma de tres partes importantes:

http://mexplaza.com.mx:80/Cencar/bienvenidos.html

- **Protocolo:** Este indica la forma con la cual nuestro navegador se comunicara con el servidor. Existen varios tipos de protocolos como: HTTP, FTP, GOPHER, NEWS, TELNET el protocolo HTTP, es el mas usado ya que este nos conecta con Páginas WWW.

- **Dirección del Servidor:** Esta puede ser el nombre de servidor o la dirección numérica del mismo, como ya quedo explicado en el apartado anterior.

  Puerto: Este dato comúnmente se encuentra definido por omisión (80), es posible que alguna dirección de un servidor WWW requiera cambiar el valor del puerto.

- **Ruta a la Información:** Este es la localización de los documentos dentro del servidor WWW.

4.- Dominios en Internet

El dominio de más alto nivel del nombre de una máquina es la serie de letras que se encuentran al extremo derecho de la dirección, y se le conoce como dominio raíz. El dominio raíz indica el tipo de organización o país a la que dicha dirección pertenece. Con este dominio, el usuario puede intuir a que tipo de organización o país pertenece la maquina a la que se está conectando.

No todos los nodos de Internet tienen la misma estructura de dirección y nombre, en algunos lugares se acostumbra a tener nombres más cortos para hacer referencia a alguna computadora, por ejemplo:

tribunalesagrarios.gob.mx

A) Dominios por países

Como dijimos anteriormente, podemos conocer el sitio donde se encuentra físicamente una maquina, fijándonos sí, en el último nivel de su dirección cuenta con un dominio que nos indica un país del mundo. Cada país se representa por dos caracteres de acuerdo con el código internacional de los países, según los estándares de la ISO (*International Standard Office).* De tal manera que si vemos una dirección como esta: usuario@prueba.es sabríamos este usuario se que se encuentra en España. La ISO 3166 nos señala cuales serán las letras por países.[369]

---

369 ISO 3166 es un estándar que codifica los nombres de países y áreas dependientes y sus principales subdivisiones.

- ISO 3166-1, códigos para países y áreas dependientes, publicado por primera vez en 1974.
  - ISO 3166-1 alfa-2, códigos de países de 2 letras.
  - ISO 3166-1 alfa-3, códigos de países de 3 letras.
  - ISO 3166-1 numérico, códigos de países de 3 números.
- ISO 3166-2, códigos de las principales subdivisones de países o áreas dependientes.
- ISO 3166-3, códigos sustitutos de los *ISO 3166-1 alfa-2* que han quedado obsoletos.

Podemos consultar la lista completa en la siguiente dirección: ***Wikipeida, La enciiopeida libre:*** http://es.wikipedia.org/wiki/ISO_3166-1

B) Dominios de Organizaciones

Existen además otras divisiones para los dominios de más alto nivel que fueron las primeras divisiones que hubo en Estados Unidos para diferenciar el tipo de organización que se conectaba a la red.

IV.- Cómo se transmite la Información en Internet.

Cuando se transmite una información en Internet (un fichero, un correo electrónico...) no se hace de una sola vez sino que se divide esa información en paquetes pequeños. De esta forma se pueden transmitir información de cualquier tamaño y se impide que las líneas por las que circula la información (líneas telefónicas, líneas de fibra óptica...) no estén colapsadas por un sólo usuario durante demasiado tiempo.

Estos paquetes están formados por la información real que se quiere transmitir y las direcciones IP de los ordenadores de origen y destino. Para llegar a su destino (que puede estar en la otra parte del mundo) estos paquetes atraviesan un cierto número de ordenadores y otros dispositivos con unas características especiales que hace que no se pierda la información.

Las distintas partes que forman Internet están conectadas por unos ordenadores llamados *routers* que se encargan de dirigir la información que reciben para que llegue a su destino. El protocolo IP se encarga de etiquetar cada paquete con la dirección IP apropiada.

Finalmente, el otro ingrediente que hace posible la comunicación entre ordenadores es el protocolo de control de transmisión TCP. Es el encargado de dividir la información en paquetes del tamaño adecuado, de numerarlos para que puedan volver a unirse en orden correcto y añadir cierta información extra para la transmisión y decodificación.

V.- Servicios y Recursos proporcionados por Internet.

Internet abarca una serie de facilidades tecnológicas que no solamente podemos englobar en la búsqueda de información o recepción de correo electrónico, Internet nos facilita otro tipo de servicios, que deberán ser debidamente explicados. Los servicios que podemos utilizar desde un ordenador conectado a Internet son muy diversos. Podemos definir servicio como un conjunto de programas y utilidades que nos permiten realizar una determinada tarea.

1.- Correo Electrónico (*Electronic-mail, email*)

Este es uno de los servicios más frecuentes dentro de Internet. Nos permite enviar mensajes (y/o ficheros) como si de correo postal se tratara, pero con la diferencia de que se recibirán inmediatamente después de mandarlos y prácticamente nunca se pierde.

Cada usuario de la red dispone de una *dirección electrónica* como ya lo estudiamos, que le identifica en todo Internet (el equivalente postal lo tenemos con nuestra dirección particular). Un ejemplo de dirección electrónica es **jimenezgl@yahoo.com.**[370] Estas direcciones se basan en la misma estructura de las direcciones IP y nombres de dominio analizados anteriormente. La única diferencia es el símbolo @ **(arroba)**[371] que se encarga de enlazar el "quién" con el "dónde" de la dirección. En este caso, sería el usuario con nombre "jimenezgl" correspondiente a la máquina "yahoo.com".

El correo electrónico, también llamado *email*, permite la comunicación entre usuarios físicamente distantes, en un período de tiempo muy corto. Y a pesar de que una llamada telefónica puede ponerlo en contacto mucho más rápido, el *email* le permite enviar y recibir gran cantidad de información de tal manera que se pueda almacenar, imprimirla o utilizarla como entrada para algunos programas. El correo electrónico también permite dejar mensajes, aún cuando el destinatario no pueda leerlo inmediatamente.

Es un sistema que permite enviar y recibir mensajes desde un ordenador a otro. Como el correo convencional, cada mensaje lleva su correspondiente dirección de destino y su remitente. De esta manera, cuando enviamos un mensaje, éste viaja desde nuestro ordenador hasta el del destinatario pasando por multitud de ordenadores intermedios los cuales van transmitiendo el mensaje hasta su destino final.

Este servicio es usado por, aproximadamente, el 60% de los usuarios de la red. Con un coste telefónico bajo, ya que con una llamada local podemos estar en contacto con una persona en el lugar más remoto del planeta lo que permite competir con el fax ya que posibilita el envío de ficheros de trabajo (y otros también) vinculados al mensaje. Además es un servicio gratuito; existen empresas nacionales y extranjeras que ofrecen gratis el servicio de correo electrónico.[372]

Al momento de contratar una conexión de Internet con un Proveedor de Servicios Internet, este nos asignará, conforme a nuestras preferencias, la dirección de *e-mail*. Todos los mensajes que recibamos mediante este sistema, se ubicaran en nuestro buzón del centro servidor a la espera que los recojamos.

---

[370]Esta es la dirección de correo electrónico del que elabora esta investigación.

[371]Hoy en día por todos lados la vemos, es un símbolo que se ha convertido en sinónimo de Internet y de los negocios electrónicos, pero no siempre fue así, hace 30 años la arroba solamente se utilizaba para algunas cartas comerciales. Es en 1971 cuando la arroba empezó su "carrera" gracias a Ray Tomlinson, científico de la empresa de investigación Bolt, Beranek and Newman (BBN), quien ayudó de forma prácticamente anónima a cambiar el mundo. Ya que fue Tomlinson el que inventó el e-mail. Para separar el nombre del dominio había que escoger un símbolo y Tomilson escogió la arroba "El signo de arroba fue incidental. Tenía que usar algo para separa ambas cosas, pero pudo haber sido cualquier otra cosa", recordó Tomlinson en una entrevista a la revista Zine Zone. "La razón para escoger la arroba, principalmente fue su escaso uso. Hacía falta un caracter que no pudiera ser parte de ningún nombre" Jose Antonio Chavez, ***La @ omnipresente***, en ***Reforma*** sección Interfase, Lunes 30 de agosto de 1999.

[372]Las recomendaciones de correo electrónico en español gratuito son: www.yahoo.com.mx, de España, www.starmedia.com, que es latinoamericano, www.correoweb.com que es de México, mail.infosel.com también mexicano, en los Estados Unidos está el multicitado www.hotmail.com, www.yahoo.com/mail y www.gmail.com, podemos acceder a cualquiera de estos sitios y obtener gratuitamente un buzón de correo electrónico. Jose E. Melo de Razo, ***Tenga un e-mail alterno,*** El Universal, Universo de la Computación, Lunes 21 de junio de 1999, pág 4.

Un mensaje de correo electrónico está formado por las siguientes partes:

- Origen o remitente (quien envía el mensaje)
- Destinatario (dirección *email* del destinatario)
- Tema (breve descripción del contenido del mensaje)
- Fecha y hora en la cual se realiza el envío (la aplicación de *email* lo pone automáticamente
- Cuerpo del mensaje
- Características (urgente, acuse de recibo,...)
- Vínculos (ficheros vinculados que se mandan con el mensaje)

Particularidades del correo electrónico

A) Copias carbón

Permite enviar una copia del mensaje que enviamos a otros destinatarios sin que el destinatario normal ni los otros lo sepan a no ser que así lo indiquemos.

B) Transferencia de mensajes

Permite reenviar un mensaje que hemos recibido a otro destinatario sin que el emisor lo sepa.

C) Listas de Distribución

Mediante el programa de correo electrónico podemos crear listas de distribución que contengan direcciones de *email* de diferentes personas que puedan estar interesadas o que nos interese que reciban un mismo mensaje. En este caso, sólo enviaremos un único mensaje a una dirección *email* que será la lista de distribución. El mensaje en cuestión lo recibirán todos los inscritos en la lista. Es preciso aclarar que se necesita de nuestro consentimiento para recibir este tipo de correo, si no es así se esta violentando nuestro derecho a la vida privada en Internet, e incluso podemos hablar del envió de *spam* o *junk mail*.

D) Seguridad del Correo Electrónico

Un mensaje cuando viaja por la red, puede ser interceptado por alguno de los administradores de los diferentes nodos por los que pasa, por lo tanto, no hay ninguna garantía de que el mensaje que nos ha llegado no haya sido manipulado. Afortunadamente, muchas aplicaciones de correo electrónico incorporan sistemas de seguridad y control y, además, los centros servidores ya han adoptado medidas contra el correo no deseado. Cabe recordar que cuando enviamos un mensaje, éste se fracciona en diferentes partes que viajan por caminos diferentes hasta llegar a su destino, donde se unen formando un único mensaje.

E) *Netiquette*[373]

Son unas reglas, no escritas, de riguroso cumplimiento por parte de los usuarios de correo electrónico y de *newsgroups* o grupos de noticias. Esta reglamentación "informal" ha surgido como un sistema de cortesía y respeto entre los diferentes usuarios. Las más significativas son:

- Hay que leer frecuentemente el correo recibido y responder lo más rápido que se pueda a los mensajes que requieran respuesta.
- Brevedad en el contenido de los mensajes.
- No enviar a listas de distribución, generalmente agrupadas por temas, mensajes que no tengan nada en común con el objetivo por el cual se ha creado la lista.
- Usar los *emoticones* o *smileys* para indicar estados emocionales o resaltar el contenido de una frase del mensaje.
- Usar el signo > cuando transcribamos literalmente parte del contenido de un mensaje que estamos respondiendo.
- Evitar, siempre que sea posible, el uso de acentos, de la ñ o de la ç, sobretodo si el mensaje lo tienen que leer personas residentes en otros países. No escribir nada en mayúsculas ya que estas solo se usan para expresar gritos.
- Vigilar las expresiones que usamos ya que alguna escrita dentro de una frase, para darle un tono irónico, puede ser malinterpretada por cualquier destinatario que provenga de una cultura diferente a la nuestra.

F) *Emoticones* o *smileys*

Son figuras muy esquemáticas creadas con los símbolos del teclado, las cuales hemos de "leer" inclinando la cabeza hacia la izquierda. Quieren expresar el espíritu mediante el cual se ha escrito un mensaje o una parte del mismo.

Como podemos observar, las *nettiquettes*, son las primeras normativas que surgen de manera espontánea entre los usuarios de Internet, como una necesidad de mantener el orden y la correcta utilización de la tecnología, podríamos decir que estás normas, son una forma de autorregulación de la red, y que no son suficientes, pero si son un ejemplo de lo que una comunidad madura puede lograr en pro del establecimiento de una organización regulada.

En conclusión podemos afirmar que este servicio de Internet es de los más usados y por ende donde podremos encontrar abundantes cuestiones jurídicas importantes en materia de protección a la vida privada.

---

[373] La **Netiquette**, palabra derivada del francés *etiquette* (buena educación) y del inglés *net* (red) o *network*, es el conjunto de reglas que regulan el comportamiento de un usuario en un grupo de noticias (newsgroup), una lista de correo (mailing list), un foro de discusiones (forum) o correo electrónico (e-mail). ***Wikipedia, La enciclopedia libre***, http://es.wikipedia.org/wiki/Netiqueta

2.- Protocolo de Transferencia de Archivos, FTP (*File Transfer Protocol*)

FTP es el protocolo de Internet que permite conectarnos a ordenadores remotos y acceder a los ficheros que guardan para trasladarlos a nuestro ordenador o, a la inversa. Un ejemplo son los libros descargables de la Biblioteca Jurídica Virtual[374] del Instituto de Investigaciones Jurídicas de la UNAM, que se encuentran en un formato de visualización pdf.

La mayoría de estos ficheros contienen programas de dominio público, utilidades, *drivers* o simplemente ficheros de texto sobre diferentes temas. Cuando capturamos un fichero, generalmente estará comprimido en formato auto extraíble o en formato ZIP[375] y, por lo tanto, será necesario que dispongamos del correspondiente descompresor que, evidentemente encontraremos por la red.

Existen servidores de Universidades, compañías informáticas, empresas que ofrecen todo tipo de ficheros que van desde *drivers* hasta programas completos, pasando por documentos y otros elementos.

Obviamente, los programas que podremos conseguir a través de estos servidores no serán nunca de carácter comercial. Podremos encontrar programas de coste compartido, *shareware*, y programas de dominio público, *freeware*.

Otro dato a destacar es el hecho de que casi todos los ficheros que circulan por la red tienen formato *comprimido*. Esto acelera las transmisiones y ahorra el espacio de disco de los servidores.

Existen otras formas de transferir archivos entre computadoras, como son los bbs y el *email*. La diferencia entre todos estos consiste en que con *email* hay un destinatario conocido cuando se envían los archivos, con los bbs y ftp no existe ese destinatario específico, los archivos están ahí para quien esté interesado en ellos, de tal manera que puedan copiarlos a sus computadoras. Existe una cantidad impresionante de archivos, tanto textos como programas, sobre muy diversos temas.

*3.- Grupos de noticias (*newsgroups*)*

Son lugares dentro de Internet en los que tiene lugar diversas "charlas"[376] o "tertulias". Podemos imaginarnos un tablón de anuncios en el que diversas personas van dejando mensajes sobre diversos temas. Cada uno puede llegar y

---

[374] ***Biblioteca Jurídica Virtual***, Instituto de Investigaciones Jurídicas, UNAM, http://www.bibliojuridica.org/

[375] Formato ZIP.- Los documentos **ZIP** o **zip** en informática son un formato de almacenamiento muy utilizado para la compresión de datos como imágenes, música, programas o documentos. ***Wikipedia, La enciclopedia libre***, http://es.wikipedia.org/wiki/Formato_de_compresi%C3%B3n_ZIP

[376] No confundir con el *chat*, ya que el grupo de noticias, es un serie de tablones donde "*posteamos*" respuestas para quien pregunta o ampliamos un tema, el cual queda dentro de un espacio determinado y no es efímero como la comunicación vía *chat*, que será estudiado más adelante.

pegar su mensaje. Los demás lo podrán ver y si es de su interés contestar con otro apunte que se añadirá en el tablón. Finalmente, los mensajes irán caducando con el paso del tiempo.[377]

Se trata de grupos públicos, ordenados por jerarquías, donde todo el mundo puede escribir sobre lo que quiera y todo el mundo puede leerlo. Estos "forúms" son ideales para preguntar dudas, comentar noticias, estar siempre al día de esa materia que nos interesa. En Internet hay una gran cantidad de conferencias públicas diarias, se estima que en torno a 70 Mb de mensajes.

4.- *Gopher*

Gopher nació en los primeros años de la década de los 90 en la Universidad de Minessota en los Estados Unidos de América y tomó el nombre de una ardilla que habita en los campos cercanos a esa universidad. Se puede decir que ha tenido una vida muy corta ya que con la aparición de las *web's*, al igual que otros servicios, actualmente se usa muy poco.

Es un sistema de consulta disponible en Internet. Se estructura de forma jerárquica, muy similar a la de un árbol de directorios de un disco duro de cualquier ordenador

Este servicio nació en respuesta a los problemas que existían en Internet a la hora de encontrar información o recursos. Funciona presentando en la pantalla un menú de opciones cuyos títulos dan una idea clara de lo que contiene. Para conectarse a un servidor *Gopher* también necesitamos un programa especial cliente *Gopher*.

Actualmente este recurso se encuentra en vías de extinción y casi absolutamente en desuso.

5.- Verónica.

Se trata de otra herramienta para buscar información. Dado que los servidores *Gopher* empezaron a proliferar se tuvo la necesidad de crear un instrumento que permitiera localizar de una manera eficaz la información dentro de los mismos. Así surgieron los servidores llamados Verónica (*Very Easy Rodent Oriented Netwide Index to Computerized Archives*).

---

[377] **Arqueólogo (Internet)** Generalmente un **"arqueólogo de Internet"**, revive un post antiguo e innecesario con el único fin de llamar la atención o provocar, interfiriendo así en el correcto desarrollo de los mismos; o simplemente por la falta de atención al publicar una respuesta, de forma compulsiva, sin detenerse en mirar la fecha original.
Se considera esta práctica contraria a la Netiqueta, y sus practicantes se sitúan muy cerca del límite de lo que sería un Troll de Internet, (en la terminología de Internet, un ***troll*** (a veces trol) es una persona que busca intencionadamente interrumpir las discusiones en Internet (por ejemplo en foros) o enfadar a sus participantes, para lo que suele usar mensajes groseros, ofensivos o fuera de tema con la intención de provocar la reacción de los demás. La palabra también se usa para describir dichos mensajes) si bien es cierto y hay que tener en consideración que en ocasiones estos desenterramientos son llevados a cabo por usuarios inexpertos e inocentes; sin que su acto haya sido hecho deliberadamente para afectar el funcionamiento del foro u otro medio de Internet.
En cualquier caso los Administradores, Sysops, moderadores , etc. dependiendo el tipo de foro, se encuentran al acecho generalmente para cerrar y enterrar, esta vez sí, definitivamente los mensajes que no necesitan ser nuevamente revividos.
http://es.wikipedia.org/wiki/Arque%C3%B3logo_%28Internet%29

6.- World Wide Web.

Es un sistema basado en hipertexto que facilita la navegación por Internet. Pero, no sólo es hipertexto, es también hipermedia ya que permite acceder a información en formato multimedia (sonido, video, etc.) *WWW* ha revolucionado la red al integrar todas las posibilidades de los otros servicios de la red que anteriormente hemos citado, en un único sistema de navegación.

El *www* es un proyecto original del CERN (Laboratorio Europeo de Física de Partículas, en Ginebra). En un principio fue creado para uso interno de esta institución pero pronto salió al exterior para convertirse en la forma más popular de acceder a la información de Internet.

Para los ordenadores personales tipo PC o Macintosh la mejor aplicación *web* que hay es *Netscape Navigator* ya que es el cliente *web* más completo, rápido y fiable, está pensado para poder ser utilizado para cualquier tipo de conexión y servicio. Le sigue en importancia *Microsoft Explorer* y ya, muy alejado se encuentra el primer cliente *web*: *Mosaic*. También los conocemos como software de *browser* o navegadores.

Una aplicación práctica de lo que hemos aprendido en este capítulo es que se puede obtener el programa mediante **FTP** en la misma red, se descomprime y se ejecuta el instalador. Una vez configurado está listo para entrar al mundo virtual del *www* simplemente introduciendo la dirección de destino y pulsar la tecla. A partir de aquí, usando el ratón iremos moviéndonos por las diferentes páginas buscando la información deseada. En pocos minutos, podremos dar la vuelta al mundo. Todo esto es posible gracias al sistema hipermedia y al lenguaje HTML.

Una de las últimas novedades del *www* y de *Netscape Navigator* son los llamados *plug ins* que no son otra cosa que extensiones del mismo programa que permiten nuevas prestaciones: visualizar gráficos en 3D, realidad virtual, escuchar la radio en directo.[378]

WWW utiliza el sistema de direcciones llamado URL (*Universal Resource Locator*) que no es más que otra forma de denominar a las direcciones IP, como ya lo estudiamos.

A) Arquitectura del World Wide Web.

El WWW responde a un modelo "*cliente-servidor*". Se trata de un paradigma de división del trabajo informático en el que las tareas se reparten entre un número de clientes que efectúan peticiones de servicios de acuerdo con un protocolo, y un número de servidores que responden a estas peticiones. En el

[378]En nuestro país podemos encontrar varias estaciones de radio en directo como ***Radio Centro*** en el AM con la dirección electrónica: http://www.radiocentro.com.mx/. O en FM, ***Reactor, todas las alternativas*** en la dirección: http://www.reactor105.imer.com.mx

web los clientes demandan hipertextos a los servidores. Para desarrollar un sistema de este tipo ha sido necesario:

a) Un nuevo protocolo que permite saltos hipertextuales, es decir, de un nodo origen a otro de destino, que puede ser texto, imágenes, sonido, animaciones, vídeo, etc. Este protocolo se denomina **HTTP** (*HiperText Transfer Protocol*) y es el lenguaje que hablan los servidores.

b) Inventar un nuevo lenguaje para representar hipertextos que incluyera información sobre la estructura y formato de representación y, especialmente, indicara el origen y destinos de los saltos de hipertexto. Este lenguaje es el **HTML** (*HyperText Markup Language*).

c) Idear una forma de codificar las instrucciones para los salto hipertextuales de un objeto a otro de la Internet (algo vital dado el caos anterior)

d) Desarrollar *aplicaciones cliente* para todo tipo de plataformas y resolver el problema de cómo se accede a la información que está almacenada, y que ésta sea disponible a través de los diversos protocolos (FTP, HTTP, WAIS...) y que representen a su vez información multiformato (texto, imágenes, animaciones, etc.). Con este fin aparecen varios clientes, entre los que destacan *Mosaic* del *NCSA* (Universidad de Chicago),[379] el *Netscape Navigator* de *Netscape Communications Corporation*[380] y el *Internet Explorer* de Microsoft.[381]

B) Conceptos Básicos del WWW.

Un protocolo de comunicación es aquél que permite que las máquinas se comuniquen entre sí, siguiendo un orden, para intercambiar e interpretar información. El protocolo que los servidores y clientes WWW usan para comunicarse se llama Protocolo de Transferencia de Hipertexto (HTTP, HyperText Transfer Protocol). Todos los servidores y clientes WWW deben ser capaces de entender este protocolo a fin de enviar y recibir documentos hipermedia. Por esto, a los servidores WWW se les llama frecuentemente servidores HTTP.

---

[379] *Mosaic*, fue el primer navegador gráfico disponible para visualizar páginas *web*. Fue creado en el NCSA en enero de 1993 por Marc Andreessen y Eric Bina. La primera versión funcionaba sobre sistemas Unix, pero fue tal su éxito que en agosto del mismo año se crearon versiones para Windows y Macintosh. *Mosaic* fue la base para las primeras versiones de Mozilla y Spyglass (más tarde adquirido por Microsoft y renombrado Internet Explorer). *Mosaic* era capaz de acceder a servicios *web* mediante HTTP, en su versión primitiva (HTTP 0.9) como la concebio Tim Berners-Lee, el cual desarrolló parte del código (acceso mediante protocolo file://, entre otros), aparte de *Gopher*, FTP y Usenet News mediante NNTP. Mosaic era software copyright de The Board of Trustees of the University of Illinois (UI). Su última versión *windows, NCSA Mosaic v3.0*, data de 1996. Nunca llegó a ser capaz de renderizar imágenes PNG, aunque sí era capaz de hacerlo en los muy comunes JPEG y GIF. El lenguaje para documentos *web* que interpretaba se corresponde con HTML2. En enero de 1997 se abandonó oficialmente el desarrollo de este navegador. Información de ***Wikipedia, La enciclopedia libre***. http://es.wikipedia.org/wiki/Mosaic

[380] Para descargar la versión 7.2 de *Netscape Navigator* se puede acceder al siguiente sitio: http://browser.netscape.com/ns8/download/archive72x.jsp

[381] Se puede obtener la versión más actual del navegador de Microsoft, el Internet Explorer 7.0, en la página de Internet siguiente: http://www.microsoft.com/spain/windows/products/winfamily/ie/default.mspx

El lenguaje estándar que "entiende" el WWW para crear y reconocer documentos de hipertexto es el HTML (Hypertext Markup Language), utilizado para crear páginas de WWW.

Es posible representar cualquier archivo o servicio en Internet con un URL. De esta manera, las ligas pueden hacerse no solamente a otros textos y medios, sino también a otra red o servicios. El éxito del World Wide Web es la facilidad que se tiene para navegar sin la necesidad de aprender comandos complicados. Únicamente se necesita conocer el manejo de un ambiente gráfico de ventanas y del ratón.

7.- Cuartos de Plática. IRC (*Internet Relay Chat*)

Es un sistema de multiconferencia creado a finales de 1988. Permite que diferentes usuarios mantengan conversaciones (por escrito) en grupos temáticos (o canales) que pueden ser privados o públicos. Por toda la red hay diferentes servidores IRC que están interconectados entre sí mediante los cuales, los usuarios de este servicio, se ponen en contacto.

Por regla general cada usuario se identifica con un *nickname* o apodo que tiene que ser único dentro del grupo.

Para usar este servicio es necesario tener instalado el correspondiente programa (*WSIRC* o el de *Netscape*). Cuando se accede a éste, aparecen los canales abiertos a los cuales podemos acceder (dependerá de nuestro servidor) con el permiso del moderador de cada uno de ellos o bien, tendremos la posibilidad de abrir nuevos canales de comunicación. Esto permite que en una sesión de IRC podamos estar "metidos" en diferentes conversaciones.

Este es el lugar ideal para conocer personas de muchísimas partes del mundo o para mantenernos en contacto con alguna persona que este fuera del país. El IRC es muy similar al sistema de radio banda (*ham radio*) en donde cada quien tiene un sobrenombre y sintoniza una frecuencia (canal) deseada e inmediatamente tiene una conversación con quien se encuentre en ese mismo canal. El inglés es el lenguaje más utilizado en IRC, sin embargo puede encontrarse con canales de otros lenguajes como español, francés o japonés.

VI.- Los navegadores, aplicaciones de navegación o *browsers*.

Los navegadores o visualizadores son programas que permiten acceder al World Wide Web, la parte gráfica de Internet. El primer navegante, llamado NCSA *Mosaic,* fue desarrollado en el *National Center for Supercomputing Applications* hace tan sólo unos pocos años. El interfaz gráfico muy sencillo de usar a través de punteros popularizó el Web, aunque sólo unos pocos podían imaginar el crecimiento tan explosivo que ocurriría.

Los navegadores permiten a los usuarios "viajar" a cualquier sitio dentro de Internet. A través de las direcciones y nombres que cada computadora en

Internet tiene asignados, el navegador puede entrar a los equipos de cómputo conectados a Internet y mostrar la información que ellos ofrecen, a través de una pantalla gráfica que despliega texto, imágenes, sonido, vídeo y multimedia.

Aunque están disponibles una gran cantidad de visualizadores diferentes, *Microsoft Explorer* y *Netscape Navigator* se llevan todos los honores. Además, son los dos únicos visualizadores que permiten acceder a todos los servicios de Internet explicados con anterioridad. Netscape y Microsoft han invertido tanto dinero en sus respectivos navegantes que la competencia no puede mantenerse a su ritmo. La encarnizada lucha entre las dos compañías para dominar el mercado ha conducido a mejoras continuas en los programas.

Los navegantes poseen todo tipo de opciones. Podríamos literalmente escribir un libro sobre cada uno de estos programas, pero el fin de la presente investigación no es convertirnos en expertos en programación sino únicamente saber como utilizar los programas que al fin y al cabo serán nuestra herramienta para generar, intercambiar, desechar, admitir toda clase de datos personales en Internet. Así daremos una pronta explicación de su uso:

La fila de botones en la parte superior del visualizador, conocida como barra de herramientas, le ayuda a viajar a través de una telaraña de posibilidades, incluso guardando un informe de los lugares en los que ha estado. Debido a que las barras de *Navigator y Explorer* son ligeramente diferentes, describiremos primero lo que hacen los botones comunes:

- El botón atrás (*back*) le devuelve a las páginas que ya ha visto.
- Use el botón adelante (*forward*) para volver a aquella página de nuevo.
- El botón principal (*principal*) le lleva a la página principal que haya elegido. (Si no ha elegido ninguna, le devolverá a la página principal por defecto, por lo general, las páginas corporativas de Microsoft o Netscape).
- Actualizar (*refresh*) hace exactamente eso, carga la página de Web de nuevo. ¿Por qué querría hacer esto? A veces, no se cargan todos los elementos de una página la primera vez, debido a que la conexión se interrumpió. También cuando carga una página de Web, la información es guardada, lo que significa que se mantiene en su computadora de manera temporal. La siguiente vez que quiera cargar esa página, en vez de solicitar el archivo al servidor, el visualizador accede directamente a la copia guardada. Pero si la página en cuestión es actualizada a menudo, como puede ocurrir con las noticias, resultados de deportes o datos bursátiles, no encontrará la información más actual. Actualizando la página, esta información se renueva.
- Imprimir (*print*) le permite obtener una copia en papel del documento actualmente cargado en su navegante.
- Finalmente, el botón parar (*stop*) le impide al visualizador terminar de cargar la página actual.

Botones únicos en Navigator:

- Puede desconectar la carga de imágenes que se cargan cuando usted accede a una página de Web. Debido a que los archivos gráficos son grandes, la página aparecerá más rápido si se trata sólo de texto. Si después decide que quiere ver las imágenes, pulse sobre el botón gráficos (*graphics*).
- El botón Abrir (*open*) le permite cargar una página de Web que usted haya podido guardar en el disco duro de su computadora. (Con Explorer, puede encontrar esta opción en el menú Archivo).
- Buscar (*search*) le permite encontrar palabras concretas dentro de un documento.

Botones únicos en Explorer:

- Búsqueda (*search*) conecta con una página en el servidor de Microsoft que ofrece una lista de directorios y recursos Internet.
- Favoritos (*favorites*) es el lugar donde guardar las direcciones de las páginas que quiere visitar de nuevo. (En Navigator, esta opción se llama Marcadores y se encuentra en la barra de Menú).
- Fuente (*font size*) le permite cambiar el tamaño del texto en la página de Web. Cada pulsación del botón aumenta el tamaño entre cuatro opciones.

Así podemos terminar diciendo que los navegadores más comunes tienen las siguientes características:

- Se distribuye gratuitamente por las compañías autorizadas, como quedo asentado en las notas al pie 20 y 21.
- Visualiza simultáneamente texto e imágenes.
- Soportan audio y video.
- Permiten realizar conexiones FTP, Http, Verónica y Gopher.

VII.- Búsquedas en Internet.

La característica de Internet es la gran cantidad de información que en ella se encuentra, información que puede ser útil para algunos y puede representar basura para otros. De nada serviría tener tal cantidad de datos sin programas que ayuden a encontrar la información que es útil a determinada persona.

Dentro de Internet existen varios servidores de búsquedas de información que ayudan al usuario a encontrar información específica[382]. Los servidores de

[382]Dos expertos del Instituto de Investigaciones de NEC en Princeton, Steve Lawrence y Lee Giles realizaron un estudio que revelaba que ningún buscador tenía clasificado más del 16% del contenido de la Red. El único que realmente llegaba a ese 16% era Northern Light (www.northernlight.com). Con los 800 millones de páginas que se estima tiene Internet - y los "mas de 3 millones " que se agregan diariamente, según Lawrence- no sorprende que los buscadores no se den abasto con su tarea. Señalando que en cuanto a amplitud el mejor buscador en la Red es el Fast Search (www.alltheweb.com) y otra herramienta útil es el **"meta"** motor capaz de interrogar varios buscadores a la vez en el cual destaca Metacrawler: www.metacrawler.com. Jay Dougherty, ***¿Cómo hallar una aguja en un pajar?***, Reforma sección Interfase, Lunes 30 de agosto de 1999.

búsquedas sólo funcionan con páginas Web, es decir, solo buscan información en el Web, aunque en la actualidad los sitios en Internet depositan su información más relevante en servidores Web.

Para buscar información dentro de Internet basta conectarse a alguno de estos servidores[383] y especificar la o las palabras de búsqueda para que el servidor muestre en la página los sitios encontrados. El nuevo término de moda es "portal"[384], ya que cada uno de estos buscadores quiere ser la puerta de entrada a la Red, el lugar donde los usuarios se detengan y echen una ojeada antes de decidir a dónde más ir una vez que se han conectado. Un portal es un lugar dónde la gente busca información.

Algunos servidores de búsqueda clasifican su información en diferentes tópicos dependiendo del tema al que se haga referencia. Estos servidores buscan dentro de las páginas que tienen registradas. Cualquier usuario puede registrar su página siguiendo las instrucciones de cada servidor de búsquedas.

1.- Búsquedas simples.

Las búsquedas simples son aquellas en las que el usuario pide que se haga una búsqueda a través de una palabra clave. El servidor devuelve todos los sitios de Internet en los cuales encontró la palabra que el usuario especificó.

2.- Búsquedas Avanzadas

Este tipo de búsqueda se realiza para encontrar documentos páginas Web con temas más específicos y en menos tiempo. Las palabras claves son combinadas de diferente forma para encontrar un documento que su contenido se refiera a un tema específico o una idea en particular.

Muchos "buscadores" cuentan con paginas especiales para este tipo de búsqueda, donde usando palabras como *and, or, not* entre otras nos permiten combinar términos para representar una idea o tema. Algunos otros cuentan con caracteres especiales como "", * ,$ -,+ para realizar búsquedas con frases, términos con diferentes forma de escribir.

Algunos buscadores cuentan con una página especial donde se puede realizar búsquedas de tipo avanzado seleccionando de algunos menús la forma en combinar los términos a buscar.

VIII.- Evolución histórica de Internet.

---

[383] Para conectarse a alguno de estos servidores, bastará saber la dirección de los más comunes, teclearla en el recuadro de abrir y comenzar la búsqueda. Las direcciones que a continuación mencionamos son las de los principales servidores de búsqueda: Yahoo: www.yahoo.com. Altavista: www.altavista.com. Google: www.google.com. En español tenemos a los buscadores: www.mexico.com, www.adnet.com y por último: http://espanol.yahoo.com

[384] La palabra surgió cuando los desarrolladores de Internet, se dieron cuenta que el espacio cibernético podría tener lugares equivalentes a plazas públicas, distritos de negocios o centros comerciales al proporcionar lugares a donde la gente recurriría primero a fuerza de costumbre. Peter Wayner, ***Abren "portales" a la Red***, Reforma sección Interfase, Lunes 13 de julio de 1998.

Internet ha supuesto una revolución sin precedentes en el mundo de la informática y de las comunicaciones. Los inventos del telégrafo, teléfono, radio y ordenador sentaron las bases para esta integración de capacidades nunca antes vivida. Internet es a la vez una oportunidad de difusión mundial, un mecanismo de propagación de la información y un medio de colaboración e interacción entre los individuos y sus ordenadores independientemente de su localización geográfica.

Conocer el desarrollo histórico de Internet es fundamental, para así comprender como esta invención ha revolucionado a nuestro entorno actual y para posteriormente dilucidar como afecta a la vida jurídica dicho fenómeno, en particular la protección de la vida privada en este medio. El no conocer la verdad histórica no nos permite entender las realidades vigentes, dentro de ese estudio observamos como nace en la Unión Americana, principal centro tecnológico mundial, su posterior globalización y un apartado específico a su aparición en el entorno nacional, analizando su situación actual de una manera ágil a través de estadísticas y gráficas.

IX.- Una breve historia de Internet

Existe actualmente una gran cantidad de material sobre la historia, tecnología y uso de Internet. Un paseo por casi cualquier librería nos descubrirá un gran número de estanterías con material escrito sobre Internet; en la biblioteca "Antonio Caso" de nuestra Facultad de Derecho de la UNAM, encontramos cerca de doce títulos referentes al tema.

Internet representa uno de los ejemplos más exitosos de los beneficios de la inversión sostenida y del compromiso de investigación y desarrollo en infraestructuras informáticas. El gobierno, la industria y el mundo académico han sido copartícipes de la evolución y desarrollo de esta nueva y excitante tecnología.

Esta historia gira en torno a cuatro aspectos distintos. Existe una evolución tecnológica que comienza con la primitiva investigación en conmutación de paquetes, ARPAnet[385] y tecnologías relacionadas en virtud de la cual la investigación actual continúa tratando de expandir los horizontes de la infraestructura en dimensiones tales como escala, rendimiento y funcionalidades de alto nivel. Hay aspectos de operación y gestión de una infraestructura operacional global y compleja. Existen aspectos sociales, que tuvieron como consecuencia el nacimiento de una amplia comunidad de internautas trabajando juntos para crear y hacer evolucionar la tecnología. Y finalmente, el aspecto de comercialización que desemboca en una transición enormemente efectiva desde los resultados de la investigación hacia una infraestructura informática ampliamente desarrollada y disponible, que ha creado nuevas formas de hacer negocios y de promover los mismos, situación que en nuestro país esta apenas en una etapa embrionaria, fértil por si misma

[385]Consultar el Glosario anexo al final del trabajo, dónde se encontrará la definición referida.

para realizar estudios de las implicaciones jurídicas que estas interacciones traerán como consecuencias.

Internet hoy en día es una infraestructura informática ampliamente extendida. Su primer prototipo es a menudo denominado *National Global or Galactic Information Infrastructure* (Infraestructura de Información Nacional Global o Galáctica). Su historia es compleja y comprende muchos aspectos: tecnológico, organizacional y comunitario. Y su influencia alcanza no solamente al campo técnico de las comunicaciones computacionales sino también a toda la sociedad en la medida en que nos movemos hacia el incremento del uso de las herramientas *online* para llevar a cabo el comercio electrónico, principal herramienta en el mundo de los negocios virtuales, la adquisición de información, herramienta clave para todo abogado que pretenda incluirse dentro de los procesos globalizadores y la acción en comunidad, que nos invita a buscar una convivencia sana y bajo un marco jurídico regulatorio de todas las actividades llevadas a cabo en la red.

1.- Los años sesenta. Orígenes de Internet

La historia de Internet podemos decir que comenzó en los principios de los años sesenta, pero para ello es necesario que nos remontemos unos años atrás, más precisamente 1957, cuando la Unión Soviética había lanzado el satélite Sputnik.[386] Se estaba en plena guerra fría, y Estados Unidos quería tener la seguridad de estar a la cabeza de la tecnología militar. En este ambiente, el Departamento de Defensa de Estados Unidos, cayó en la cuenta de que la tecnología empleada por la red telefónica tradicional, era demasiado frágil para resistir el más mínimo ataque, y mucho menos la tan temida guerra nuclear. Si se destruían una conexión entre dos centrales importantes quedaba una central fuera de servicio, buena parte de las telecomunicaciones de defensa del país podrían quedar inutilizadas. En 1962 Paul Baran,[387] un investigador del gobierno de Estados Unidos, editó el libro sobre las redes de comunicación distribuidas,(*On Distributed Communications Networks*) donde se describen las redes de conexión entre ordenadores. Este proyecto daba una solución a la interrogante planteada por el Departamento de Defensa, Baran propuso un sistema de comunicación mediante ordenadores conectados en una red descentralizada. De manera que si uno o varios nodos importantes eran destruidos, los demás podían comunicarse entre sí sin ningún inconveniente.

La primera descripción documentada acerca de las interacciones sociales que podrían ser propiciadas a través del *networking* (trabajo en red) está contenida en una serie de memorándums escritos por J.C.R. Licklider,[388] del

---

[386]El Sputnik, fue el primer satélite puesto en órbita, media 23 pulgadas de diámetro, por 86 pulgadas de largo incluyendo sus antenas hechas de aluminio pulido. En Octubre 4 de 1957 fue puesto en órbita, realizando 1,400 recorridos, finalmente fue incinerado en la atmósfera en Enero 4 de 1958. Información obtenida de la ***Enciclopedia Encarta 2007, disponible en CD-Rom.***

[387]BARAN, Paul, ***On Distributed Communications Networks,*** IEEE Trans. Comm Sys. Estados Unidos de América, Marzo de 1962.

[388]LICKLIDER, J.C.R., y W. CLARK, ***On- Line Man-Computer Communication, Agosto 1962 en Proceeding of the IEEE,*** Edición especial de Comunicaciónes de redes mediante paquetes, volúmen 66, N° 11, Estados Unidos de América, Enero 1972.

Massachusetts Institute of Technology, en Agosto de 1962, en los cuales Licklider discute sobre su concepto de *Galactic Network* (Red Galáctica). El concibió una red interconectada globalmente a través de la que cada uno pudiera acceder desde cualquier lugar a datos y programas. En esencia, el concepto era muy parecido a la Internet actual. Licklider fue el principal responsable del programa de investigación en ordenadores de la DARPA[389] desde Octubre de 1962. Mientras trabajó en DARPA convenció a sus sucesores Ivan Sutherland, Bob Taylor, y el investigador del MIT Lawrence G. Roberts de la importancia del concepto de trabajo en red.

En Julio de 1961 Leonard Kleinrock[390] publicó desde el MIT el primer documento sobre la teoría de conmutación de paquetes. Kleinrock convenció a Roberts de la factibilidad teórica de las comunicaciones vía paquetes en lugar de circuitos, lo cual resultó ser un gran avance en el camino hacia el trabajo informático en red. El otro paso fundamental fue hacer dialogar a los ordenadores entre sí. Para explorar este terreno, en 1965, Roberts conectó un ordenador TX2 en Massachusetts con un Q-32 en California a través de una línea telefónica conmutada de baja velocidad, creando así la primera (aunque reducida) red de ordenadores de área amplia jamás construida. El resultado del experimento fue la constatación de que los ordenadores de tiempo compartido podían trabajar juntos correctamente, ejecutando programas y recuperando datos a discreción en la máquina remota, pero que el sistema telefónico de conmutación de circuitos era totalmente inadecuado para esta labor. La convicción de Kleinrock acerca de la necesidad de la conmutación de paquetes quedó confirmada.

A finales de 1966 Roberts se trasladó a la DARPA a desarrollar el concepto de red de ordenadores y rápidamente confeccionó su plan para ARPANET, publicándolo en 1967.[391] En la conferencia en la que presentó el documento se exponía también un trabajo sobre el concepto de red de paquetes a cargo de Donald Davies y Roger Scantlebury del NPL. Scantlebury le habló a Roberts sobre su trabajo en el NPL así como sobre el de Paul Baran y otros en RAND. El grupo RAND había escrito un documento sobre redes de conmutación de paquetes para comunicación vocal segura en el ámbito militar, en 1964. Ocurrió que los trabajos del MIT (1961-67), RAND (1962-65) y NPL (1964-67) habían discurrido en paralelo sin que los investigadores hubieran conocido el trabajo de los demás. La palabra *packet* (paquete) fue adoptada a partir del trabajo del NPL y la velocidad de la línea propuesta para ser usada en el diseño de ARPAnet fue aumentada desde 2,4 Kbps hasta 50 Kbps.[392]

---

[389] La *Advanced Research Projects Agency* (ARPA, Agencia de Proyectos de Investigación Avanzada) cambió su nombre a *Defense Advanced Research Projects Agency* (DARPA, Agencia de Proyectos de Investigación Avanzada para la Defensa) en 1971, más tarde retomó su antigua denominación de ARPA en 1993, para volver a DARPAen 1996. Nosotros la llamaremos siempre con su nombre actual DARPA.

[390] KLEINROCK, L., ***Information Flow in Large Communications Nets***, RLE Quarterly Progress Report, Estados Unidos de America, Julio de 1961.

[391] ROBERTS,L., ***Multiple Computer Networks and Intercomputer Communications;*** Conferencia de la Association for Computer Machinery en Gatlinburg, Octubre de 1967.

[392] Fue a partir del estudio de RAND como se inició el rumor de que ARPAnet era algo relacionado con la construcción de una red resistente a la guerra nuclear. En realidad, en la historia oficial esto nunca fue cierto. Solamente el estudio de RAND sobre seguridad vocal tomaba en consideración la guerra nuclear. Sin embargo, el trabajo posterior en

En Agosto de 1968, después de que Roberts y la comunidad de la DARPA hubieran refinado la estructura global y las especificaciones de ARPAnet, DARPA lanzó un RFQ (*Request for Comments*, petición de comentarios) para el desarrollo de uno de sus componentes clave: los conmutadores de paquetes[393] llamados *Interface message processors* (IMPs, procesadores de mensajes de interfaz). El RFQ fue ganado en Diciembre de 1968 por un grupo encabezado por Frank Heart, de Bolt Beranek y Newman (BBN). Así como el equipo de BBN trabajó en IMPs con Bob Kahn tomando un papel principal en el diseño de la arquitectura de la ARPAnet global, la topología de red y el aspecto económico fueron diseñados y optimizados por Roberts trabajando con Howard Frank y su equipo en la Network Analysis Corporation, y el sistema de medida de la red fue preparado por el equipo de Kleinrock de la Universidad de California, en Los Angeles.[394]

A causa del temprano desarrollo de la teoría de conmutación de paquetes de Kleinrock y su énfasis en el análisis, diseño y medición, su *Network Measurement Center* (Centro de Medidas de Red) en la UCLA (Universidad de California Los Angeles) fue seleccionado para ser el primer nodo[395] de ARPAnet. Todo ello ocurrió en Septiembre de 1969, cuando BBN instaló el primer IMP en la UCLA y quedó conectado el primer ordenador *host*. El proyecto de Doug Engelbart denominado *Augmentation of Human Intelect* (Aumento del Intelecto Humano) que incluía NLS, un primitivo sistema hipertexto en el Instituto de Investigación de Standford (SRI) proporcionó un segundo nodo. El SRI patrocinó el *Network Information Center*. Un mes más tarde, cuando el SRI fue conectado a ARPAnet, el primer mensaje de *host* a *host* fue enviado desde el laboratorio de Leinrock al SRI. Se añadieron dos nodos en la Universidad de California, Santa Bárbara, y en la Universidad de Utah. Estos dos últimos nodos incorporaron proyectos de visualización de aplicaciones, con Glen Culler y Burton Fried en la UCSB

Así, a finales de 1969, cuatro ordenadores *host* fueron conectados conjuntamente a la ARPAnet inicial y se hizo realidad una embrionaria Internet. Incluso en esta primitiva etapa, hay que reseñar que la investigación incorporó tanto el trabajo mediante la red ya existente como la mejora de la utilización de dicha red. Esta tradición continúa hasta el día de hoy.

Los comienzos de Arpanet y de Internet en la comunidad de investigación universitaria estimularon la tradición académica de la publicación abierta de

---

Internetting hizo énfasis en la robustez y capacidad de supervivencia, incluyendo la capacidad de resistir la pérdida de grandes porciones de redes en uso.

[393]Mediante la conmutación de paquetes, toda la información que sale de una terminal para ser transmitida por la red es troceada en bloques de una determinada longitud llamados paquetes (*paquets*). A cada paquete se le añade una información adicional al comienzo del mismo, formando lo que se llama una cabecera. En la cabecera va la información necesaria (identificativos del terminal origen y destino entre otras cosas), para que cada paquete se pueda mover por la red de forma independiente. Si en un momento dado una ruta o un nodo de comunicaciones queda fuera de servicio, los paquetes que en principio utilizaban estos medios son enviados de forma automática por otras rutas, sin que quede interrumpida la comunicación. Como veremos más adelante esta red experimental contaba con apenas unos cuatro nodos, una cifra risible si se considera que en la actualidad se estiman más de 48,000 nodos.

[394]Dentro del equipo de Kleinrock, destacan Vinton Cerf, Steve Crocker y Jon Postel. Más tarde se unieron a ellos David Crocker que jugó un importante papel en la documentación de los protocolos de correo electrónico y Robert Braden que desarrolló los protocolos de comunicación para los grandes ordenadores IBM.

[395]Ver Glosario anexo.

Ideas y resultados. Sin embargo, el ciclo normal de la publicación académica tradicional era demasiado formal y lento para el intercambio dinámico de ideas, esencial para crear redes.

En 1969 S.Crocker,[396] entonces en UCLA, dio un paso clave al establecer la serie de notas RFC (*Request For Comments*, petición de comentarios). Estos memoranda pretendieron ser una vía informal y de distribución rápida para compartir ideas con otros investigadores en redes. Al principio, las RFC fueron impresas en papel y distribuidas vía correo "lento". Pero cuando el FTP (*File Transfer Protocol*, protocolo de transferencia de ficheros) empezó a usarse, las RFC se convirtieron en ficheros difundidos *online* a los que se accedía vía FTP. Hoy en día, desde luego, están disponibles en el World Wide Web en decenas de emplazamientos en todo el mundo.

El efecto de las RFC era crear un bucle positivo de realimentación, con ideas o propuestas presentadas a base de que una RFC impulsara otra RFC con ideas adicionales y así sucesivamente. Una vez se hubiera obtenido un consenso se prepararía un documento de especificación. Tal especificación sería entonces usada como la base para las implementaciones por parte de los equipos de investigación.

El acceso abierto a las RFC –libre si se dispone de cualquier clase de conexión a Internet- promueve el crecimiento de Internet porque permite que las especificaciones sean usadas a modo de ejemplo en las aulas universitarias o por emprendedores al desarrollar nuevos sistemas.

El *email* o correo electrónico ha supuesto un factor determinante en todas las áreas de Internet, lo que es particularmente cierto en el desarrollo de las especificaciones de protocolos, estándares técnicos e ingeniería en Internet. Las primitivas RFC a menudo presentaban al resto de la comunidad un conjunto de ideas desarrolladas por investigadores de un solo lugar. Después de empezar a usarse el correo electrónico, el modelo de autoría cambió: las RFC pasaron a ser presentadas por coautores con visiones en común, independientemente de su localización.

2.- Los años setenta. Los protocolos TCP/IP.

Se siguieron conectando ordenadores rápidamente a la ARPAnet durante los años siguientes, ARPAnet había crecido hasta 15 nodos con 23 ordenadores centrales y el trabajo continuó para completar un protocolo *host* a *host* funcionalmente completo, así como software adicional de red. En Diciembre de 1970, el *Network Working Group* (NWG) liderado por S.Crocker acabó el protocolo *host* a *host* inicial para ARPAnet, llamado *Network Control Protocol* (NCP, protocolo de control de red). Cuando en los nodos de ARPANET se completó la implementación del NCP durante el periodo 1971-72, los usuarios de la red pudieron finalmente comenzar a desarrollar aplicaciones.

---

[396] ***RFC001, Host Software,*** Estados Unidos de Norteamérica, 7 de abril de 1969. Primer *Request For Comments*, petición de comentarios, existente en la red.

En Octubre de 1972, Kahn organizó una gran y muy exitosa demostración de ARPAnet en la *International Computer Communication Conference*. Esta fue la primera demostración pública de la nueva tecnología de red. Fue también en 1972 cuando se introdujo la primera aplicación "estrella": el correo electrónico. En Marzo, Ray Tomlinson, de BBN, escribió el software básico de envío-recepción de mensajes de correo electrónico, impulsado por la necesidad que tenían los desarrolladores de ARPAnet de un mecanismo sencillo de coordinación. En Julio, Roberts expandió su valor añadido escribiendo el primer programa de utilidad de correo electrónico para relacionar, leer selectivamente, almacenar, reenviar y responder a mensajes. Desde entonces, la aplicación de correo electrónico se convirtió en la mayor de la red durante más de una década. Fue precursora del tipo de actividad que observamos hoy día en la *World Wide Web*, es decir, del enorme crecimiento de todas las formas de tráfico persona a persona.

Es en el año de 1973 cuando se dan las primeras conexiones internacionales producto de la conferencia internacional de comunicación entre ordenadores, siendo el *College London* de Inglaterra y el *Royal Radar Establishment*, en Noruega, junto con los ahora 37 nodos de expansión en ARPAnet era muy fácil conectarse debido a su estructura descentralizada.

En 1974 se estableció el *Transmission Control Protocol* (TCP) creado por Vinton Cerf y Bob Kahn desarrollándose hasta convertirse en el *Transmission Control Protocol/Internet Protocol (TCP/IP).* Para llegar a esta unificación de protocolos se tuvo que desarrollar toda una arquitectura de redes que se llamó *internetting*, que es fundamental explicar a grosso modo como se desarrollaron los protocolos descritos.

La ARPAnet original, evolucionó hacia Internet. Internet se basó en la idea de que habría múltiples redes independientes, de diseño casi arbitrario, empezando por ARPAnet como la red pionera de conmutación de paquetes, pero que pronto incluiría redes de paquetes por satélite, redes de paquetes por radio y otros tipos de red. Internet como ahora la conocemos encierra una idea técnica clave, la de arquitectura abierta de trabajo en red. Bajo este enfoque, la elección de cualquier tecnología de red individual no respondería a una arquitectura específica de red sino que podría ser seleccionada libremente por un proveedor e interactuar con las otras redes a través del metanivel de la arquitectura de *Internetworking* (trabajo entre redes).

En una red de arquitectura abierta, las redes individuales pueden ser diseñadas y desarrolladas separadamente y cada una puede tener su propia y única interfaz, que puede ofrecer a los usuarios y/u otros proveedores, incluyendo otros proveedores de Internet. Cada red puede ser diseñada de acuerdo con su entorno específico y los requerimientos de los usuarios de aquella red. No existen generalmente restricciones en los tipos de red que pueden ser incorporadas ni tampoco en su ámbito geográfico, aunque ciertas consideraciones pragmáticas determinan qué posibilidades tienen sentido. La idea de arquitectura de red abierta fue introducida primeramente por Kahn un

poco antes de su llegada a la DARPA en 1972. Este trabajo fue originalmente parte de su programa de paquetería por radio, pero más tarde se convirtió por derecho propio en un programa separado. Entonces, el proyecto fue llamado *Internetting* que surgió con la necesidad no solamente de contar con un protocolo de comunicaciones seguro, sino también de contar con un protocolo que permitiese interconectar distintas redes entre sí. Kahn pensó primero en desarrollar un protocolo local sólo para la red de paquetería por radio porque ello le hubiera evitado tratar con la multitud de sistemas operativos distintos y continuar usando NCP.

Sin embargo, NCP no tenía capacidad para direccionar redes y máquinas más allá de un destino IMP en ARPAnet y de esta manera se requerían ciertos cambios en el NCP. La premisa era que ARPAnet no podía ser cambiado en este aspecto. En este modelo, el NCP no tenía control de errores en el *host* porque ARPAnet había de ser la única red existente y era tan fiable que no requería ningún control de errores en la parte de los *hosts*.

Así, Kahn decidió desarrollar una nueva versión del protocolo que pudiera satisfacer las necesidades de un entorno de red de arquitectura abierta. El protocolo podría eventualmente ser denominado *"transmision-control protocol/Internet protocol"* (TCP/IP, protocolo de control de transmisión /protocolo de Internet). Así como el NCP tendía a actuar como un *driver* (conductor) de dispositivo, el nuevo protocolo sería más bien un protocolo de comunicaciones.

Cuatro fueron las reglas fundamentales en las primeras ideas de Kahn:

- ☐ Cada red distinta debería mantenerse por sí misma y no deberían requerirse cambios internos a ninguna de ellas para conectarse a Internet.

- ☐ Las comunicaciones deberían ser establecidas en base a la filosofía del *"best-effort"* (lo mejor posible). Si un paquete no llegara a su destino debería ser en breve retransmitido desde el emisor.

- ☐ Para interconectar redes se usarían cajas negras, las cuales más tarde serían denominadas *gateways* (escapes) y *routers* (enrutadores). Los gateways no deberían almacenar información alguna sobre los flujos individuales de paquetes que circulasen a través de ellos, manteniendo de esta manera su simplicidad y evitando la complicada adaptación y recuperación a partir de las diversas modalidades de fallo.

- ☐ No habría ningún control global a nivel de operaciones.

Kahn empezó a trabajar en un conjunto de principios para sistemas operativos orientados a comunicaciones mientras se encontraba en BBN y escribió algunas de sus primeras ideas en un memorándum interno de BBN titulado

"*Communications Principles for Operating Systems*".[397] Así, en la primavera de 1973, después de haber empezado el trabajo de "Internetting", le pidió a Vinton Cerf (entonces en la Universidad de Stanford) que trabajara con él en el diseño detallado del protocolo. Cerf había estado íntimamente implicado en el diseño y desarrollo original del NCP y ya tenía conocimientos sobre la construcción de interfaces con los sistemas operativos existentes. De esta forma, valiéndose del enfoque arqui-tectural de Kahn en cuanto a comunicaciones y de la experiencia en NCP de Cerf, se asociaron para abordar los detalles de lo que acabaría siendo TCP/IP.

El trabajo en común fue altamente productivo y la primera versión escrita[398] bajo este enfoque fue distribuida en una sesión especial del INWG (*International Network Working Group*, Grupo de trabajo sobre redes internacionales) que había sido convocada con motivo de una conferencia de la Universidad de Sussex en Septiembre de 1973. Cerf había sido invitado a presidir el grupo y aprovechó la ocasión para celebrar una reunión de los miembros del INWG, ampliamente representados en esta conferencia de Sussex.

El documento original de Cerf y Kahn sobre Internet describía un protocolo, llamado TCP, que se encargaba de proveer todos los servicios de transporte y reenvío en Internet. Kahn pretendía que TCP diera soporte a un amplio rango de servicios de transporte, desde el envío secuencial de datos, totalmente fiable (modelo de circuito virtual) hasta un servicio de datagramas en el que la aplicación hiciera un uso directo del servicio de red subyacente, lo que podría implicar pérdida ocasional, corrupción o reordenación de paquetes.

Una de las motivaciones iniciales de ARPAnet e Internet fue compartir recursos, por ejemplo, permitiendo que usuarios de redes de paquetes sobre radio pudieran acceder a sistemas de tiempo compartido conectados a ARPAnet. Conectar las dos redes era mucho más económico que duplicar estos carísimos ordenadores. Sin embargo, mientras la transferencia de ficheros y el *login* remoto (Telnet) eran aplicaciones muy importantes, de todas las de esta época probablemente sea el correo electrónico la que haya tenido un impacto más significativo. El correo electrónico[399] dio lugar a un nuevo modelo de comunicación entre las personas y cambió la naturaleza de la colaboración. Su influencia se manifestó en primer lugar en la construcción de la propia Internet (como veremos más adelante), y posteriormente, en buena parte de la sociedad.

Se propusieron otras aplicaciones en los primeros tiempos de Internet, desde la comunicación vocal basada en paquetes (precursora de la telefonía sobre

---

[397] Memorandum interno BBN. Enero de 1972.

[398] Esta fue más tarde publicada como: V.G. CERF y R. E. KAHN, ***"A Protocol for packet Network Interconnection"***, IEEE Trans. Comm. Tech., Vol. Com-22, V5, Estados Unidos de Norteamérica, Mayo de 1974, págs. 627-641.

[399] El deseo de intercambiar correo electrónico llevó, sin embargo a la aparición de uno de los primeros libros sobre Internet: ***A Directory of Electronic Mail Addressing and Networks***, de FREY y ADAMS, que tocaba el tema sobre la traducción y el envió de direcciones de correo electrónico.

Internet) o varios modelos para compartir ficheros y discos, hasta los primeros "programas-gusano" que mostraban el concepto de agente (y, por supuesto, de virus). Un concepto clave en Internet es que no fue diseñada para una única aplicación sino como una infraestructura general dentro de la que podrían concebirse nuevos servicios, como con posterioridad demostró la aparición de la *World Wide Web*. Este fue posible solamente debido a la orientación de propósito general que tenía el servicio implementado mediante TCP e IP, por eso es destacable haber reseñado la creación de estos protocolos que se convierten en espina dorsal de el desarrollo de Internet, ya que posteriormente cuando aparecieron los ordenadores personales, TCP era demasiado grande y complejo para funcionar en ordenadores personales. Así David Clark y su equipo de investigación del MIT empezaron a buscar la implementación de TCP más sencilla y compacta posible. La desarrollaron, primero para el Alto de Xerox (la primera estación de trabajo de Xerox) y luego para el Personal Computer de IBM. Esta implementación abriría las puertas a los ordenadores personales, demostrando que las estaciones de trabajo, al igual que los grandes sistemas, podían ser parte de Internet.

El crecimiento de ARPAnet hizo necesario la creación de algunos órganos de gestión: el Internet Configuration Control Board fue formado por la DARPA en 1979. Más tarde se transformó en el Internet Activities Board y en la actualidad es el Internet Architecture Board Society.

3.- Los años ochenta. La transición hacia una infraestructura global

En los años 80, el desarrollo de LAN,(*Local Area Networks*, Redes locales de area) PC (*Personal Computer,* Computadora Personal) y estaciones de trabajo permitió que la naciente Internet floreciera. La tecnología Ethernet, desarrollada por Bob Metcalfe en el PARC de Xerox en 1973, es la dominante en Internet, y los PCs y las estaciones de trabajo los modelos de ordenador dominantes. El cambio que supone pasar de unas pocas redes con un modesto número de hosts (el modelo original de ARPAnet)) a tener muchas redes dio lugar a nuevos conceptos y a cambios en la tecnología. En primer lugar, hubo que definir tres clases de redes (A, B y C) para acomodar todas las existentes. La clase A representa a las redes grandes, a escala nacional (pocas redes con muchos ordenadores); la clase B representa redes regionales; por último, la clase C representa redes de área local (muchas redes con relativamente pocos ordenadores).

Como resultado del crecimiento de Internet, se produjo un cambio de gran importancia para la red y su gestión. Para facilitar el uso de Internet por sus usuarios se asignaron nombres a los *hosts* de forma que resultara innecesario recordar sus direcciones numéricas. Originalmente había un número muy limitado de máquinas, por lo que bastaba con una simple tabla con todos los ordenadores y sus direcciones asociadas.

El cambio hacia un gran número de redes gestionadas independientemente (por ejemplo, las LAN) significó que no resultara ya fiable tener una pequeña

tabla con todos los *hosts*. Esto llevó a la invención del DNS (*Domain Name System*, sistema de nombres de dominio) por Paul Mockapetris de USC/ISI. El DNS permitía un mecanismo escalable y distribuido para resolver jerárquicamente los nombres de los *hosts* (por ejemplo, *www.unam.mx* o *www.derecho.unam.mx*) en direcciones de Internet.

El incremento del tamaño de Internet resultó también un desafío para los *routers*. A medida que el número de redes en Internet se multiplicaba, el diseño inicial no era ya capaz de expandirse, por lo que fue sustituido por un modelo jerárquico de enrutamiento con un protocolo IGP (*Interior Gateway Protocol*, protocolo interno de pasarela) usado dentro de cada región de Internet y un protocolo EGP (*Exterior Gateway Protocol*, protocolo externo de pasarela) usado para mantener unidas las regiones.

A medida que evolucionaba Internet, la propagación de los cambios en el software, especialmente el de los *hosts*, se fue convirtiendo en uno de sus mayores desafíos. DARPA financió a la Universidad de California en Berkeley en una investigación sobre modificaciones en el sistema operativo Unix, incorporando el TCP/IP desarrollado en BBN. Visto en perspectiva, la estrategia de incorporar los protocolos de Internet en un sistema operativo utilizado por la comunidad investigadora fue uno de los elementos clave en la exitosa y amplia aceptación de Internet.

Uno de los desafíos más interesantes fue la transición del protocolo para *hosts* de ARPAnet desde NCP a TCP/IP el 1 de enero de 1983. Se trataba de una ocasión muy importante que exigía que todos los *hosts* se convirtieran simultáneamente o que permanecieran comunicados mediante mecanismos desarrollados para la ocasión. La transición fue cuidadosamente planificada dentro de la comunidad con varios años de antelación a la fecha, pero fue sorprendentemente sobre ruedas (a pesar de dar la lugar a la distribución de insignias con la inscripción "Yo sobreviví a la transición a TCP/IP").

TCP/IP había sido adoptado como un estándar por el ejército norteamericano tres años antes, en 1980. Esto permitió al ejército empezar a compartir la tecnología DARPA basada en Internet y llevó a la separación final entre las comunidades militares y no militares. En 1983 ARPAnet estaba siendo usada por un número significativo de organizaciones operativas y de investigación y desarrollo en el área de la defensa. La transición desde NCP a TCP/IP en ARPAnet permitió la división en una MILnet para dar soporte a requisitos operativos militares y una ARPAnet para las necesidades de investigación.

Así, en 1985, Internet estaba firmemente establecida como una tecnología que ayudaba a una amplia comunidad de investigadores y desarrolladores, y empezaba a ser empleada por otros grupos en sus comunicaciones diarias entre ordenadores. El correo electrónico se empleaba ampliamente entre varias comunidades, a menudo entre distintos sistemas. La interconexión entre los diversos sistemas de correo demostraba la utilidad de las comunicaciones electrónicas entre personas.

Al mismo tiempo que la tecnología Internet estaba siendo validada experimentalmente y usada ampliamente entre un grupo de investigadores de informática se estaban desarrollando otras redes y tecnologías. La utilidad de las redes de ordenadores (especialmente el correo electrónico utilizado por los contratistas de DARPA y el Departamento de Defensa en ARPAnet) siguió siendo evidente para otras comunidades y disciplinas de forma que a mediados de los años 70 las redes de ordenadores comenzaron a difundirse allá donde se podía encontrar financiación para las mismas. El Departamento norteamericano de Energía (DoE, *Deparment of Energy*) estableció MFEnet para sus investigadores que trabajaban sobre energía de fusión, mientras que los físicos de altas energías fueron los encargados de construir HEPnet. Los físicos de la NASA continuaron con SPAN y Rick Adrion, David Farber y Larry Landweber fundaron CSnet para la comunidad informática académica y de la industria con la financiación inicial de la NFS (*National Science Foundation*, Fundación Nacional de la Ciencia) de Estados Unidos. Todas las primeras redes (como ARPAnet) se construyeron para un propósito determinado. Es decir, estaban dedicadas (y restringidas) a comunidades cerradas de estudiosos; de ahí las escasas presiones por hacer estas redes compatibles y, en consecuencia, el hecho de que durante mucho tiempo no lo fueran. Además, estaban empezando a proponerse tecnologías alternativas en el sector comercial, como XNS de Xerox, DECNet, y la SNA de IBM. Sólo restaba que los programas ingleses JANET (1984) y norteamericano NSFNET (1985) anunciaran explícitamente que su propósito era servir a toda la comunidad de la enseñanza superior sin importar su disciplina. De hecho, una de las condiciones para que una universidad norteamericana recibiera financiación de la NSF para conectarse a Internet era que "la conexión estuviera disponible para *todos* los usuarios cualificados del campus". [400]

En 1985 Dennins Jenning acudió desde Irlanda para pasar un año en NFS dirigiendo el programa NSFnet. Trabajó con el resto de la comunidad para ayudar a la NSF a tomar una decisión crítica: si TCP/IP debería ser obligatorio en el programa NSFnet.

Se hizo la selección de TCP/IP para el programa NSFnet como obligatorio lo que dio como consecuencia que las agencias federales norteamericanas idearon y pusieron en práctica otras decisiones que llevaron a la Internet de hoy:

- ☐ Las agencias federales compartían el coste de la infraestructura común, como los circuitos trans-oceánicos. También mantenían la gestión de puntos de interconexión para el tráfico entre agencias: los "Federal Internet Exchanges"

- ☐ Para coordinar estas actividades se formó el FNC (*Federal Networking Council*, Consejo Federal de Redes).[401] El FNC cooperaba también con

---

[400] ***Rules of Financiation of the National Science Foundation,*** National Science Foundation, Estados Unidos de Norteamerica, 1984, págs. 27-28.

[401] Denominado originalmente FRICC (***Federal Research Internet Coordinating Committee***, Comité de Coordinación Federal de Investigación sobre Internet)

otras organizaciones internacionales, como RARE en Europa, a través del CCIRN (*Coordinating Committee on Intercontinental Research Networking*, Comité de Coordinación Intercontinental de Investigación sobre Redes) para coordinar el apoyo a Internet de la comunidad investigadora mundial.

- Esta cooperación entre agencias en temas relacionados con Internet tiene una larga historia. En 1981, un acuerdo sin precedentes entre Farber, actuando en nombre de CSNET y NSF, y Kahn por DARPA, permitió que el tráfico de CSNET compartiera la infraestructura de ARPAnet de acuerdo según parámetros estadísticos.

- En consecuencia, y de forma similar, la NFS promocionó sus redes regionales de NSFnet, inicialmente académicas, para buscar clientes comerciales, expandiendo sus servicios y explotando las economías de escala resultantes para reducir los costes de suscripción para todos.

- En el *backbone* NFSnet (el segmento que cruza la espina dorsal) NSF estableció una política aceptable de uso (AUP, *Acceptable-Use Policy*) que prohibía el uso del *backbone* para fines "que no fueran de apoyo a la Investigación y la Educación". El predecible e intencionado resultado de promocionar el tráfico comercial en la red a niveles locales y regionales era estimular la aparición y/o crecimiento de grandes redes privadas y competitivas como PSI, UUNET, ANS CO+RE, y, posteriormente, otras. Este proceso de aumento de la financiación privada para el uso comercial se resolvió tras largas discusiones que empezaron en 1988 con una serie de conferencias patrocinadas por NSF en la *Kennedy School of Government* de la Universidad de Harvard, bajo el lema "La comercialización y privatización de Internet", complementadas por la lista "*com-priv*" de la propia red.

- En 1988 un comité del *National Research Council* (Consejo Nacional de Investigación), presidido por Kleinrock y entre cuyos miembros estaban Clark y Kahn, elaboró un informe dirigido a la NSF y titulado *"Towards a National Research Network"*. El Informe llamó la atención del entonces senador Al Gore[402] le introdujo en las redes de alta velocidad que pusieron los cimientos de la futura «Autopista de la Información».

- La política de privatización de la NSF culminó en Abril de 1995 con la eliminación de la financiación del backbone NSFnet. Los fondos así recuperados fueron redistribuidos competitivamente entre redes regionales para comprar conectividad de ámbito nacional a Internet a las ahora numerosas redes privadas de larga distancia.

[402]Hay que destacar que Al Gore fue vicepresidente de los Estados Unidos de Norteamérica desde 1992 hasta 2000 cuando busco la presidencia de su país y ha sido uno de los principales precursores de la Política Informática durante la administración Clinton.

El *backbone* había hecho la transición desde una red construida con *routers* de la comunidad investigadora (los *routers* Fuzzball de David Mills) a equipos comerciales. En su vida de ocho años y medio, el *backbone* había crecido desde seis nodos con enlaces de 56Kb a 21 nodos con enlaces múltiples de 45Mb.Había visto crecer Internet hasta alcanzar más de 50.000 redes en los cinco continentes y en el espacio exterior, con aproximadamente 29.000 redes en los Estados Unidos.

El efecto del ecumenismo del programa NSFnet y su financiamiento (200 millones de dólares entre 1986 y 1995) y de la calidad de los protocolos fue tal que en 1990, cuando la propia ARPAnet se disolvió, TCP/IP había sustituido o marginado a la mayor parte de los restantes protocolos de grandes redes de ordenadores e IP estaba en camino de convertirse en *el* servicio portador de la llamada Infraestructura Global de Información.

4.- Los años noventa. Historia del Futuro.

Como ya analizamos, ARPAnet como entidad se extinguió en 1990, habiendo sobrepasado objetivos y metas que tenía en su origen. Los usuarios de la red apenas lo notaron, , ya que las funciones de ARPAnet no solamente continuaron, sino que mejoraron notablemente a través de nuevos órganos más representativos de la utilización actual de la red.

El crecimiento del mundo empresarial trajo como consecuencia un incremento de la preocupación por el propio proceso de crecimiento de la red. Desde los primeros años de la década de los ochentas, hasta hoy, Internet creció y está creciendo más allá de sus raíces originales de investigación para incluir a una amplia comunidad de usuarios y una actividad comercial creciente. Se puso un mayor énfasis en hacer el proceso abierto y justo. Esto, junto a una necesidad reconocida de dar soporte a la comunidad de Internet, condujo a la formación de la *Internet Society* en el año también de 1991, bajo los auspicios de la CNRI (*Corporation for National Research Initiatives,* Corporación para las iniciativas de Investigación Nacionales) de Kahn y el liderazgo de Cerf, junto al de la CNRI.

A medida que la red fue creciendo, empezaron a integrarse algunos usuarios que tenían escasos conocimientos en materia de computación. Por tal motivo fue necesario diseñar nuevas y más sencillas herramientas de comunicación para Internet. Uno de los primeros pasos lo dio la Universidad de Minnesota en 1991, con la creación de un programa que permite revisar directorios y obtener archivos mediante un sencillo sistema de menús. El ménu es una lista jerárquica de opciones que permite seleccionar con el teclado o el *mouse* alguna de ellas, la que a su vez puede presentar otra lista de opciones sin límite de niveles. Ese programa que fue llamado gopher, facilitó considerablemente el acceso a Internet, porque permitió accesar recursos en otros formatos, incluyendo gráficas y sonidos. Rápidamente el uso de gopher se extendió por

todo el mundo y diversas instituciones comenzaron a ofrecer su propio servicio, como lo es Verónica[403], hasta formar una red mundial apoyada en Internet.

En este mismo año, el mayor centro de Internet en Europa era el CERN (*European High Energy Particle Physics Lab*). En ese organismo, en el año de 1992 Tim Berners Lee (en la actualidad el director del *World Wide Web Consortium*), creó la World Wide Wed, utilizando tres nuevos recursos: HTML (*Hypertext Markup Languange*) HTTP (*Hypertext Transfer Protocol*) y un programa cliente llamado *Web Browser.* Todo este trabajo se basó en un escrito de Ted Nelson, en 1974, donde, por primera vez, se habló de Hypertext un nuevo lenguaje de programación y de links. La WWW es la mejor herramienta para navegar en Internet. Su éxito se debe a que permite acceder a los distintos recursos de Internet con un solo programa. La WWW es intuitiva y fácil de usar, además de amena y llena de posibilidades.

En 1992 todavía se realizó otra reorganización en las instituciones dedicadas a administrar Internet: El *Internet Activities Board* (Consejo de Actividades de Internet) fue reorganizado y sustituyó al Consejo de la Arquitectura de Internet, operando bajo los auspicios de la Internet Society. Se definió una relación más estrecha entre el nuevo IAB (*Internet Architecture Board,* Consejo de la Arquitectura de Internet) y el IESG,(*Internet Engineering Steering Group,* Grupo de Dirección de Ingeniería de Internet) tomando el IETF (*Internet Engineering Task Force,* Equipo de Trabajo de Ingeniería de Internet)y el propio IESG una responsabilidad mayor en la aprobación de estándares. Por último, se estableció una relación cooperativa y de soporte mutuo entre el IAB, el IETF y la *Internet Society,* tomando esta última como objetivo la provisión de servicio y otras medidas que facilitarían el trabajo del IETF.

En 1993, en el *National Center for Supercomputing Apliations* (NCSA), en la Universidad de Illinois, Mac Andressen junto con un grupo de estudiantes crearon un programa llamado Mosaic (osea un Web Browser), el cual ganó fama rápidamente. Mac Andressen, al poco tiempo, se alejó del NCSA y junto con Jim Clark fundaron Netscape. La idea de Andressen fue sensata; se alejaría de un lugar donde trabajaba prácticamente gratis, para crear otro que, según él , le daría enormes cantidades de dinero. Lo de Jim Clark (fundador de *Silicon Graphics*) fue apostar a todo o nada, pues se alejó de una de las empresas más prosperas de Silicon Valley, para fundar otra que no sabía si funcionaria o no, pero como podemos observar ganó la apuesta. En estos momentos Netscape es uno de los programas más utilizados en Internet como Web Browser.

El número de servidores Internet sobrepasa los dos millones. También NSF patrocina una nueva organización, InterNIC, creada para proporcionar servicios de registro en Internet y bases de datos de direcciones.

---

[403]Por sus iniciales en inglés se le conoce como Verónica: *Very Easy Rodent-Oriented Netwide Index to Computarized Archives,* consiste en un servicio que mantiene un índice de objetos *gopher,* y provee un método para realizar requerimientos sobre esos objetos.

En número de servidores de Internet alcanza los tres millones ochocientos mil servidores para 1994. Las primeras tiendas de comercio electrónico aparecen junto con "emisores" de radio *online*. El conflicto potencial entre los internautas tradicionales y los nuevos usuarios se manifestó con el tumulto que causó un gabinete legal americano que introdujo publicidad en Internet, produciendo que la misma perdiera sus dotes de investigación y universitario para pasar al ámbito del lucro y el comercio, acción que motivo el "boom" del uso del Internet. Hoy en día es difícil pensar una página *web* sin un solo anuncio publicitario en ella.

A partir de 1994 se ha vivido una nueva fase en la comercialización. Originalmente, los esfuerzos invertidos en esta tarea consistían fundamentalmente en fabricantes que ofrecían productos básicos para trabajar en la red y proveedores de servicio que ofrecían conectividad y servicios básicos. Internet se ha acabado convirtiendo en una "***commodity***",[404] un servicio de disponibilidad generalizada para usuarios finales, y buena parte de la atención se ha centrado en el uso de la GII (*Global Information Infraestructure*) para el soporte de servicios comerciales. Este hecho se ha acelerado tremendamente por la rápida y amplia adopción de visualizadores y de la tecnología del World Wide Web, permitiendo a los usuarios acceder fácilmente a información distribuida a través del mundo. Están disponibles productos que facilitan el acceso a esta información y buena parte de los últimos desarrollos tecnológicos están dirigidos a obtener servicios de información cada vez más sofisticados sobre comunicaciones de datos básicas de Internet. Así como la adquisición de bienes de consumo vía la red, lo que se ha llamado *ecommerce* o comercio electrónico, disciplina realmente novedosa ya que actualmente las tecnologías permiten este tipo de transacciones que anteriormente no eran accesibles. Podemos decir que cuando en 1990 se decidió eliminar la obligación de contar con apoyo gubernamental para poder conectarse a Internet, dio comienzo un periodo extraordinario de crecimiento de la red, gracias al inicio de las actividades comerciales a través de ésta. De 159,000 ordenadores conectados a Internet, ascendieron a un total de 4,851,000 hacia principios de 1995.

El 24 de Octubre de 1995, el FNC (*Federal Networking Council*, Consejo Federal de la Red) aceptó unánimemente una resolución definiendo el término *Internet*. La definición se elaboró de acuerdo con personas de las áreas de Internet y los derechos de propiedad intelectual. La resolución: "el FNC acuerda que lo siguiente refleja nuestra definición del término *Internet*. *Internet* hace referencia a un sistema global de información que está relacionado lógicamente por un único espacio de direcciones global basado en el protocolo de Internet (IP) o en sus extensiones, es capaz de soportar comunicaciones usando el conjunto de protocolos TCP/IP o sus extensiones u otros protocolos compatibles con IP, y emplea, provee, o hace accesible, privada o públicamente, servicios

[404]Es cualquier bien tangible. Productos como granos, metales y alimentos son "*commodities*" transados en los diferentes mercados internacionales. ***Glosario de términos financieros***, Página en Internet de Econoinvest con la dirección: http://www.econoinvest.com/glosario.aspx?sec=140326. El término nos hace referencia a la posibilidad de vender y comprar objetos tangibles vía la Internet, es decir comercio material virtual.

de alto nivel en capas de comunicaciones y otras infraestructuras relacionadas aquí descritas". También en 1995, había más de 5 millones de servidores conectados a Internet, la espina dorsal de NSFnet empezaba a ser sustituida por proveedores comerciales interconectados.

Internet estará en el centro del crecimiento y cambio del mercado de la industria de las Tecnologías de la Información y para muchas otras industrias. Para 1999 IDC[405] predice un cambio fundamental en Internet, de un ambiente limitado y ajeno a las masas, hacia uno que empieza a percibirse cada vez más como el mundo real. Por supuesto Internet no desaparecerá, se transformará, es decir, para finales de 1999, será un lugar radicalmente diferente al que ya empezábamos a acostumbrarnos.

Para los analistas de IDC, 1999 se destaco por el crecimiento acelerado y sostenido de Internet el cual llegó a los 147 millones de usuarios, alcanzando los niveles de población de países como Rusia y Japón. También se destaca el hecho de que la mayoría de los usuarios de Internet vivirán fuera de los Estados Unidos, IDC predice que, por primera vez, la mayoría (51%) de los usuarios de Internet vivirán en otros países.

Dentro de los puntos más destacados está el hecho de que, en los Estados Unidos, las mujeres serán la mayoría en la red. En 1998 las mujeres crecieron del 43% al 48% del total de la población en línea en Estados Unidos. IDC predice que en 1999 las mujeres romperán la barrera del 50%. Este es un cambio importante y clave para las empresas que hacen negocios en la red porque hasta ahora los hombres eran la mayoría en Internet. El éxito en la nueva Internet dependerá de entender las diferencias entre mujeres y hombres al usar la red: ellas buscan diferentes sitios *web*, utilizan menos tiempo para navegar y lo más importante, ellas son las que toman las decisiones de compra en la mayoría de los hogares. Es también en 1999 cuando el formato de sonido mp3 desestabiliza a las multinacionales del disco y se convierte en todo un fenómeno que cambia la cultura pop de las sociedades occidentales, junto con el aparecen paginas de descarga de música gratuita como lo es Napster y las múltiples demandas que recibe por este motivo, también nace en este año Google, el principal buscador a nivel mundial en la actualidad.

5.- Del 2000 a la fecha. Multimedia y cientos de millones de usuarios.

El nuevo siglo trajo consigo importantes y nuevos retos para Internet., en el año 2000, el famoso y sobre ponderado efecto 2000 o Y2K,[406] provoca apenas

---

[405] ***Predicciones de IDC para 1999,*** en la home page de Select-IDC México: www.select-idc.com.mx/bolpren/Predicciones IDC0199.htm

[406] El **Problema del año 2000**, también conocido como **efecto 2000 o Y2K**, es un error de software causado por la costumbre que habían adoptado los programadores al omitir los dos primeros dígitos del año para su almacenamiento (generalmente para economizar memoria), asumiendo que el software sólo funcionaría durante los años cuyos nombres comenzaran con 19. De esta manera, para estos programas, la fecha después del 31 de diciembre de 1999, sería el 1 de enero de 1900 en vez de 1 de enero de 2000. Al acercarse el año 2000, surgieron muchos rumores de caos y catástrofes económicas en el mundo entero, un pavor generalizado de un eventual colapso de los sistemas basados en

algunos problemas, El índice Nasdaq alcanza su pico histórico pero a la vez tiene un fuerte desplome, el gigante Microsoft es condenado por abusar de su cuasimonopollo en sistemas operativos, podemos decir que en estos dos primeros años del nuevo siglo comienza la era de los nuevos medios de comunicación o lo que conocemos por multimedia.[407] La compra de Tlmer Warner, una gran empresa de televisión por cable por el ISP America Online, marca el principio de este fenómeno.

En estos años se autorizan tres nuevos nombres de dominio que no van a tener éxito, el .name para personas, el .coop para cooperativas y el .aero para aeronáuticas, todo mundo sigue optando por el .com, se generaliza en el año 2002 el uso de *weblogs* o *blogger*, que son páginas de Internet escritas por los usuarios de la red para exponer sus anécdotas y dan a conocer opiniones de temas muy variados, se habla de que estamos viviendo la mayor libertad de expresión que jamás hayamos imaginado. En el 2003 la empresa de ordenadores Apple inaugura su tienda de música en formato mp3 *iTunes*, asociada con el muy exitoso reproductor en este formato *iPod*, la cual es una forma legal de obtener archivos de música que pagan los derechos de autor a los artistas.

Uno de los más importantes acontecimientos ha sido la aparición del acceso inalámbrico a Internet, lo cual ha dado más facilidad y movilidad a la comunicación, este tipo de tecnología ha creado lo que se llama las redes WiFi, un ejemplo es la RIU de la UNAM (Red Inalámbrica Universitaria)[408] que permite el uso de *laptops* y otros dispositivos móviles que puedan acceder a Internet, para que así toda la comunidad universitaria tenga acceso a este tipo de tecnología de forma gratuita. Además podemos decir que entre el 2004 y el 2005 los módems han sido superados por dispositivos de banda ancha para proveer mayor velocidad en la conexión a Internet, en 2005 la red llega a tener más de 300 millones de servidores y casi 60 millones de dominios activos y más de 4,000 millones de páginas *web* archivadas por el buscador Google y cerca de 900 millones de usuarios en el mundo, en diciembre de 2005 se alcanza la cifra de 1000 millones de usuarios en todo el mundo de los cuales 4,633,400 en México.[409] Pero no todo ha sido bueno para el desarrollo de Internet, en este año se dan ataques de *pishing*,[410] de forma generalizada y son muchas las

---

computadoras por causa de este problema. La corrección del problema costó miles de millones de dólares en el mundo entero, sin contar otros costes relacionados. ***Wikipedia, La enciclopedia libre***, http://es.wikipedia.org/wiki/Problema_del_a%C3%B1o_2000, Incluso la Unión Europea, emitió un comunicado denominado ***"El problema informático del efecto 2000"*** siendo el 98 (102), el cual incluía entre otras cosas que tanto estaba preparada la comunidad, los costos y beneficios, como solucionar el problema, finalmente los problemas fueron mínimos como ya se ha dicho, consulta del documento íntegro en: http://www.onnet.es/comy2k.pdf

[407] El experto en medios J. Quintana nos dice lo siguiente en relación a la multimedia: "En el campo de las Nuevas Tecnologías podemos acotar el concepto de multimedia al sistema que integra o combina diferentes medios: texto, imagen fija (dibujos, fotografías) sonidos (voz, música, efectos especiales) imagen en movimiento (animaciones, videos), a través de un único programa (*software*)." Es decir podemos incorporar todos los medios de comunicación, radio, televisión, computadora en un solo aparato mediante un *software*. QUINTANA, J, ***Multimèdia: què i per a què, Guix***, núm. 233, Paris, 1997, pág. 5.

[408] Para más información acceder al sitio www.riu.unam.mx

[409] La fuente fue la ***Encuesta Nacional sobre Disponibilidad y Uso de Tecnología de Información*** del INEGI, 2004.

[410] Según Koon Tan "es un término utilizado en informática con el cual se denomina el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. El estafador, mejor conocido

entidades bancarias por el mundo que sufren de este fenómeno, entre ellas Banesto, Citybank, BBVA, HSBC, el *pishing* es la capacidad de duplicar una página *web* para hacer creer al visitante que se encuentra en la página original en lugar de en la copiada. Se usa con fines delictivos o para la obtención de datos personales sensibles, así se duplican las páginas de bancos conocidos y se envían correos de forma indiscriminada para que se acceda a la página para actualizar los datos de acceso al banco y así obtener contraseñas y nombres de usuario para cometer fraudes con las cuentas de los usuarios de los servicios financieros.

Se ha afianzado en el año pasado el concepto llamado *"web 2.0"* [411]caracterizada por uso avanzado de la *web* por parte de usuarios que no se limitan a una navegación pasiva sino que comparten y producen contenidos, colaboran con otros usuarios y establecen relaciones sociales a través de Internet. Esto incluye la expansión de los videoblogs o sitios donde se comparten video clips como lo es YouTube y los *podcasts*[412] que apuntan a ser la segunda oleada de Internet.

Es un hecho que en 2006 los usuarios de Internet comenzaron a fortalecerse, la mayoría familiarizados con sitios como Google, Ebay, Yahoo y Amazon, pero su popularidad no durara para siempre, así podemos afirmar que sitios como YouTube, MySpace, Bebo, Hi5 y demás páginas comunitarias donde los usuarios pueden intercambiar contenidos serán el foco para las comunidades *online* durante el 2007, esto aunado al crecimiento en la utilización de la telefonía celular en aplicaciones de Internet, ya que dicha tecnología nos permite tener videoconferencias en tiempo real, correo electrónico y acceso a Internet casi en cualquier lugar, incluso en las estaciones del Metro de esta ciudad portando un celular de la compañía Telcel.

---

como *phisher* se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas" TAN, Koon. **Phishing and Spamming via IM (SPIM).** Internet Storm Center, 5 de diciembre del 2006

[411] El término fue acuñado por Dale Dougherty de O´Reilly Media en una lluvia de ideas con Craig Cline de MediaLive para desarrollar ideas para una conferencia. Dougherthy sugirió que Internet estaba en un renacimiento, con reglas que cambiaban y modelos de negocio que evolucionaban, la forma más fácil de entenderla es por medio de ejemplos así para la *web 1.0* la Enciclopedia Británica Online es para la *web 2.0* la Wikipedia, una enciclopedia hecha por contenidos que ingresan los usuarios en una clara participación más directa. O´REILLY, Tim, ***What is web 2.0,*** *Design Patterns and Business Models for the Next Generation of Software,* Conferencia web 2.0, San Francisco, Septiembre 30 de 2005.

[412] ***Podcast.***- consiste en crear archivos de sonido (generalmente en ogg o mp3) y distribuirlos mediante un archivo RSS de manera que permita suscribirse y usar un programa que lo descargue para que el usuario lo escuche en el momento que quiera, generalmente en un reproductor portátil. Un *podcast* se asemeja a una suscripción a un blog hablado en la que recibimos los programas a través de Internet. También una ventaja del *podcast* es la posibilidad de escuchar en lugares sin cobertura. Su contenido es diverso, pero suele ser una persona hablando sobre diversos temas. Esta es la definición base. Ahora bien, puede ser ampliada de diferentes maneras. Hay *podcasts* sobre diversos temas, sobre todo tecnológicos. Mucha gente prefiere usar un guión y otros hablan *a capella* y de forma improvisada. Algunos parecen un programa de radio, intercalando música, mientras que otros hacen *podcasts* más cortos y exclusivamente con voz, igual que con los weblogs. El término *podcasting* surge como el acrónimo de las palabras *pod* y *broadcast.* Fue sugerido por primera vez entre otros términos, por Ben Hammersley en *The Guardian* el 12 de febrero de 2004 para describir la posibilidad de escuchar audio en reproductores portátiles. Así, el término *pod* sugiere *portable device,* es decir, reproductor portátil y *broadcast,* emisión de radio o televisión. Otra acepción de "*Podcast*" es: Portable On Demand Broadcast, es decir emisión portátil a solicitud. Inicialmente referido a las emisiones desde *audioblogs,* actualmente ya es aceptado para referirse a emisiones multimedia, de video y/o audio. ***Wikipedia, La enciclopedia libre,*** http://es.wikipedia.org/wiki/Podcasting#Origen_del_t.C3.A9rmino . Cabe señalar que ya es una palabra reconocida por el Oxford English Dictionary.

El crecimiento alcanzado por la Internet en los últimos años ha sido impresionante. Para ilustrarnos en función de su crecimiento utilizaremos las estadísticas que nos proporciona la *Internet World Stats*,[413] que abarca el crecimiento de la población en la red y el crecimiento de la "triple w". Notamos en las cifras el crecimiento acelerado y como ha aumentado en porcentajes muy importantes el uso de Internet, junto con este crecimiento también se da el de los datos personales y su probable utilización sin nuestra autorización o para fines comerciales, por tanto es ahora más imperioso el proteger este derecho fundamental.

X.- Breve reseña histórica del desarrollo de Internet en México.[414]

La presencia de Internet en México aún es limitada. Comparando con todos los estudios hechos en los Estados Unidos de Norteamérica y algunos países de Europa, su presencia la podemos ubicar de manera certera en 1989, pero gracias al gran crecimiento debido al auge de Internet en el mundo hoy día podemos integrar una historia de su desarrollo en nuestro país. Desarrollo fortalecido principalmente por las instituciones de educación superior en específico la Universidad Nacional Autónoma de México y el Instituto Tecnológico de Estudios Superiores de Monterrey.

1.- El Primer Nodo Internet en México

La historia del Internet en México empieza en el año de 1989 con la conexión del Instituto Tecnológico y de Estudios Superiores de Monterrey, en el Campus Monterrey (ITESM), hacia la Universidad de Texas en San Antonio (UTSA), específicamente a la escuela de Medicina. Cabe destacar que esta institución privada de educación superior junto con la nuestra querida Universidad Nacional, han dado vida a la Informática en México y en muchos aspectos han sido iniciadores de tecnologías necesarias para el desarrollo del país, nos dice Alejandro Pisanty:[415] "... la segunda institución que toma el uso de la Informática en el país es el ITESM". En ese mismo sentido José Treviño Abrego,[416] recuerda que fue en 1963 cuando se trajo la primera computadora para apoyar sus procesos administrativos, y es en 1967, cuando un grupo de personas, entre las que se encontraba el mismo Treviño Abrego, rector del Campus "Eugenio Garza Sada" en Monterrey, se organizó para establecer formalmente, un año después la carrera de Ingeniero en sistemas computacionales.

Retomando la aparición de Internet en el país señalamos que antes de que el Instituto Tecnológico de Estudios Superiores de Monterrey se conectara a Internet, casi a final de los 80's, recibía el tráfico de BITnet por la misma línea

---

[413] Ver **Gráficos 1** del Apéndice.

[414] Para más información ver ***Una Historia que Contar MEXNET A.C.,*** ISOC México, www.isoc.com.mx y ***Revista NET@***, Vol 1, Num 19,México,1997.

[415] En artículo de LÓPEZ, Ernesto, ***De 40 años, y sigue joven***, Reforma, Sección Interfase, México, Lunes 12 de Octubre de 1998. Primera columna.

[416] En artículo de SANCHEZ, Verónica, ***Prevén mayor integración empresarial y menores costos y mejor calidad***, Reforma, Sección Interfase, México, Lunes 12 de Octubre de 1998. Página 13A.

privada. El ITESM era participe de BITnet desde 1986 y la Universidad Nacional lo era desde octubre de 1987.

Las conexiones se hacían a través de líneas conmutadas. La conexión permanente de esta institución se logró hasta el 15 de Junio de 1987 (a BITnet y posteriormente a Internet).

Nuestra Máxima casa de estudios la Universidad Nacional Autónoma de México, como ya señalamos, ha intervenido de manera importante en el desarrollo de la informática en nuestro país. Podemos destacar dos acontecimientos que la revisten como pionera en las tecnologías de la información, ya que a fines de 1958 la Universidad Nacional Autónoma de México, decidió el arrendamiento del primer sistema de cómputo comercial de IBM, el IBM 650, para utilizarlo principalmente con fines de investigación científica, y así. Podemos citar lo que nos relata Alejandro Pisanty, director general de Servicios de Computo Académico de la UNAM: "Entre 1957 y 1958, Nabor Carrillo entonces rector de la Universidad, pidió a dos científicos muy importantes, Carlos Gress y Alberto Barajas, que visitaran instituciones universitarias e industriales del área de cómputo en Estados Unidos para ver a mayor profundidad en qué consistían y qué oportunidades planteaban ya en proyectos concretos lo que en esa época se llamaba los "cerebros electrónicos", para determinar la utilidad específica que podían tener y determinar en su momento una adquisición en particular que pudiera ser útil a la universidad"[417], observamos entonces que la UNAM fue la primera institución en todo el país en poseer un equipo de computo para investigación académica, el segundo logro para la historia de la informática en México fue el conformar el segundo nodo Internet en México siendo la Universidad Nacional Autónoma de México, donde se realizara esta conexión, en específico en el Instituto de Astronomía en la Ciudad de México. Esto mediante una conexión vía satélite de 56 Kbps, con el Centro Nacional de Investigación Atmosférica (NCAR) de Boulder, Colorado, en los Estados Unidos de Norteamérica. Por lo tanto, se trataba de una línea digital.

En Noviembre de 1988 se cambia la conexión permanente que interconectaba equipo IBM con RSCS, a equipos DEC utilizando DECnet. Al cambiar el protocolo se tenía la posibilidad de encapsular tráfico de TCP/IP en DECnet y por lo tanto formar parte de Internet.

Al siguiente año, en 1989, se cambió de una a tres líneas. Con ello, se cambió el equipo de interconexión y se incorporaron los equipos de ruteo CISCO. Las conexiones siguieron siendo con la UTSA.

2.- Primeros equipos conectados a Internet

La primera máquina que recibía la conexión de DECnet esa una Microvax-II, fue el primer servidor de nombres para el dominio mx., naciendo el día 1º de

[417]En artículo de LOPEZ, Ernesto, ***De 40 años, y sigue joven***, Reforma, Sección Interfase, México, Lunes 12 de Octubre de 1998. Primera columna.

febrero de 1989, con la dirección 131.178.1.1 (desde Septiembre de 1993 se encuentra fuera de operación en el ITESM, Campus Monterrey). Esta máquina tenía un software que recibía el tráfico de TCP/IP encapsulado en DECnet, lo sacaba y permitía acceder a Internet.

Además de ser el primer nodo de Internet en México, pasó a ser el primer *Name server* para el dominio .mx, como ya lo señalamos.

Después de esto, lo que proseguía era una interconexión entre la UNAM y el ITESM (Campus Monterrey), pero lo que funcionó en ese entonces fue un enlace a BITnet entre ellos.

El ITESM, en su Campus Estado de México, se conecta a través del Centro de Investigación Atmosférica (NCAR) a Internet. Como la UNAM, obtiene una conexión satelital de 56 kbps, es decir, enlace digital. La función de este enlace es dar servicio a los demás ITESM, diseminados a través de todo el país.

3.- Conexiones posteriores

El ITESM, Campus Monterrey, promovió y logró que la Universidad de las Américas (UDLAP) en Cholula, Puebla y el Instituto Tecnológico y de Estudios Superiores de Occidente (ITESO) en Guadalajara, Jalisco, se enlazaran a Internet a través del mismo ITESM.

Aunque sus enlaces eran de baja velocidad, 9600 bps, fue suficiente, en ese momento, para proveer de correo electrónico, transferencia de archivos y acceso remoto.

Debido al crecimiento registrado en Internet, la *National Science Foundation,* en los Estados Unidos, requería de una respaldada red de telecomunicaciones para todos aquellos países que se integraban a Internet, por lo tanto, se tomaron algunas decisiones en México, como la de formalizar el uso de IGRP entre los ruteadores y revisar detalladamente la asignación de ASN (*Authonomous Systems*).

La Universidad de Guadalajara, obtiene una conexión a Internet con la Universidad de California en Los Ángeles. Esta era una línea privada de 4 hilos a 9600 bps. Estaban bajo el dominio de UCLA y con direcciones de IP también de la UCLA.

Las demás instituciones, en ese tiempo, accesaban Internet por medios conmutados. Tal es el caso de el Colegio de Postgraduados (COLPOS) de la Universidad de Chapingo, en el Estado de México. El Centro de Investigación en Química Aplicada, con sede en Saltillo, Coahuila. El Laboratorio Nacional de Informática de Xalapa, Veracruz. Todos ellos se conectaban al ITESM, Campus Monterrey para salir a Internet.

La Universidad de Guanajuato en Salamanca, Guanajuato, se enlazaba a la UNAM. El Instituto Tecnológico de Mexicali, en Baja California; se conectaba a la red de BESTnet.

4.- Formación de MEXNET

En este entonces existía un organismo llamado RED-MEX, formado principalmente por la academia, y es donde se discutía las políticas, estatutos y procedimientos que habrían de regir y dirigir el camino de la organización de la red de comunicación de datos de México. Esta debería ser una Asociación Civil.

Es así (después de muchos problemas para reunir a los representantes legales de cada institución) como surge MEXNET el lugar fue la Universidad de Guadalajara. El motivo era crear la asociación civil. El día 20 de enero de 1992 los participantes: ITESM; Universidad de Guadalajara; Universidad de las Américas; ITESO; Colegio de Postgraduados; LANIA; CIQA; Universidad de Guanajuato; Universidad Veracruzana; Instituto de Ecología; Universidad Iberoamericana; IT de Mexicali.

Más tarde, el 1ro. de Junio de 1992, MEXnet establece una salida digital de 56kbps al *backbone* de Internet.

El crecimiento de MEXnet fue registrando a usuarios como: UdeG, IPN, CINVESTAV, UAdeC, UdeM, INAOE, en 1992; UAM, UAG, Universidad Panamericana, CIMIT, UAP, UA de Chapingo, UAAAN, COMIMSA, UASLP, Universidad Veracruzana, UANL y Universidad Autónoma de Puebla entre otros, esto durante 1993.

BAJAred se empieza a formar con las siguientes instituciones educativas, todas ellas de Baja California:

- Centro de Enseñanza Técnica y Superior - CETYS.
- Centro de Investigación Científica y Educación Superior de Ensenada - CICESE.
- Universidad Autónoma de Baja California - UABC.
- Colegio de la Frontera Norte - COLEF.
- Instituto Tecnológico de Mexicali - ITM

Cabe señalar que para ese entonces no se requirió de una administración dedicada al registro de dominios, ya que no existían muchos nombres de dominio com.mx. Para el año de 1992 había sólo 45 dominios bajo .mx, de los cuales 40 eran académicos y 5 eran comerciales.

En 1993 el CONACyT se conecta a Internet mediante un enlace satelital al NCAR. El ITAM hace lo propio el 18 de Enero de 1993.

Es en 1993 cuando la UAM se establece como el primer NAP, al intercambiar tráfico entre dos diferentes redes.

Para finales de 1993 existían una serie de Redes ya establecidas en el País, algunas de ellas:

- MEXnet
- Red UNAM
- Red ITESM
- RUTyC, que desaparecería como tal ese mismo año
- BAJAnet
- Red Total CONACYT
- SIRACyT: un esfuerzo por agrupar las anteriores

Dentro de los esfuerzos de la SIRACyT se acordó crear los subdominos com.mx, gob.mx, y es en esa misma junta en la Universidad de Monterrey, donde se decide no crear el subdominio edu.mx.

Fue hasta 1994, con la formación de Red Tecnológica Nacional (RTN), integrada por MEXnet y CONACyT que el enlace creció a 2Mbps. Y es en este año que el Internet se abre a nivel comercial en nuestro país PIXELnet, ya que hasta entonces, solamente instituciones educativas y de investigación lograron realizar su enlace a Internet.

Durante 1994 y 1995, se consolidaron redes como Red Tecnológica Nacional creando un *Backbone* nacional y agrupando a un gran numero de instituciones educativas y comerciales en toda la República, desde Baja California hasta Quintana Roo. Se mantuvieron esfuerzos de la Red UNAM y surgieron los ISP's comerciales con más fuerza, los cuales no sólo brindaban conexión a Internet sino servicios de valor agregado, tales como acceso a Bases de Datos públicas y privadas.

A principios de 1995 eran poco más de 100 nombres de dominio ubicados bajo .mx.

5.- Consolidación de los servicios de Internet en México

En Diciembre de 1995 se hace el anuncio oficial del Centro de Información de Redes de México (NIC-México) el cual se encarga de la coordinación y administración de los recursos de Internet asignados a México, tales como la administración y delegación de los nombres de dominio ubicados bajo el código de dos letras asignado a cada país según el ISO 3166[418], en dónde México ocupa el dominio mx. En un primer lugar el ***Network Information Center-México,*** era dependiente del ITESM, Campus Monterrey, trabajo que venía desarrollando de manera oficial desde 1989, para febrero del 2007 hay 193,057

[418] Ver **Anexo 1** en el Apéndice de esta misma obra.

nombres de dominio con .mx a diferencia de los 326 que existían a finales de 1997.[419]

En 1996, ciudades como Monterrey, N.L., registran cerca de 17 enlaces contratados con Telmex para uso privado. Se consolidan los principales ISP's (*Internet Service Providers,* Proveedores de servicios de Internet) en el país, de los casi 100 ubicados a lo largo y ancho del territorio nacional. A finales de este año hay 2838 nombres de dominio bajo .mx.

En los primeros meses, tan sólo el 2% de los *hosts* totales (16,000) ubicados bajo .mx tienen en su nombre las letras **www**.

Nace la Sociedad Internet, Capítulo México,[420] una asociación internacional no gubernamental no lucrativa para la coordinación global y cooperación en Internet. Se crea el *Computer Emergency Response Team de México.*

A finales del 96 la apertura en materia de empresas de telecomunicaciones y concesiones de telefonía de larga distancia provoca un auge **momentáneo** en las conexiones a Internet. Empresas como Avantel (comprada el 4 de diciembre de 2006 por Axtel) y Alestra-AT&T ahora compiten con Telmex.

En 1997 existen más de 150 Proveedores de Acceso a Internet (ISP's) que brindan sus servicios en el territorio mexicano, ubicados en los principales centros urbanos: Cd. de México, Guadalajara, Monterrey, Chihuahua, Tijuana, Puebla, Mérida, Nuevo Laredo, Saltillo, Oaxaca, por mencionar sólo algunos.

El 27 de enero de 1997 se celebró el Primer Encuentro de Proveedores de Acceso a Internet y Operadores de Redes Públicas de Telecomunicaciones, en el Museo Tecnológico de la Comisión Federal de Electricidad, donde se discutieron cuestiones importantes en cuanto al uso de Internet en México, destacando el discurso inaugural del Lic. Carlos Casaús López Hermosa,[421] Presidente de la Comisión Federal de Telecomunicaciones dónde señaló: "El desarrollo de Internet, es un tema que tiene la máxima importancia para nuestro país en las vísperas del siglo XXI" y por lo tanto señala que "la globalización ha traído consigo la necesidad de integrarse a las cadenas productivas y de comercio electrónico".

En cuanto a la infraestructura nacional afirmó que: "el acceso básico en México y en todo el mundo es, hasta hoy, la red telefónica local. Nuestro país cuenta apenas con 10 teléfonos para cada 100 habitantes, lo que impide que las grandes mayorías puedan siquiera pensar en adquirir en los próximos años un acceso (a Internet) particular" y apuntó que: "Las dos redes dorsales más

---

[419] ***Estadísticas mensuales de nombres de dominio registrados bajo .mx en México,*** obtenidas del sitio de NIC México, www.nic.mx . Ver **Gráficos 2** en el Apéndice de este trabajo

[420] Ver: ***Charter for the Mexican Chapter of the Internet Society,*** December 1995 en la dirección electrónica: isocmex.org.mx/charter.html

[421] ***Discurso Inaugural en el Encuentro de Proveedores de Acceso a Internet y Operadores de Redes Públicas de Telecomunicaciones,*** que se encuentra en la dirección electrónica: http://isocmex.org/encuentro.html

importantes siguen siendo la Red Tecnológica Nacional y la Red de la Universidad Nacional Autónoma de México".

En entrevista a Alejandro Pisanty, Presidente del Capítulo México de la Internet Society y responsable de la Dirección General de Servicios de Cómputo Académico de la UNAM, afirmó que la situación de Internet en México para 1998 es muy interesante: "tenemos estimados de entre 400 y posiblemente 500 mil usuarios de Internet en el país para finales de este año. La mayor parte de los sectores consideran a Internet como un recurso valioso e imprescindible; hay gente de gran inteligencia y creatividad desarrollando servicios valiosos de Internet en México; hay instancias del gobierno que están transformando su manera de funcionar gracias a Internet"[422]

6.- El papel de NIC México en el nuevo siglo.

La evolución de NIC México ha sido toral para el desarrollo de Internet en México en lo que va del presente siglo y finales del pasado, sus políticas y tarifas para creación de dominios ha facilitado a todos los usuarios el establecer su nuevo dominio y por lo tanto tener presencia en la red.

Para 1998 nuestro país contaba con 10,000 nombres de dominio registrados y pagados lo que permite a NIC adquirir una infraestructura más robusta y confiable: Un enlace de 128K con UNINET, uno de 256K con AVANTEL y 10MB con el ITESM, Campus Monterrey; servidores SUN 450, 250, Ultra 2 y Sparc 20 y equipo de ruteo cisco 7200 y 2500. En Marzo de este mismo año se disminuyen las tarifas de registro y mantenimiento en 30%. A mediados de año el NIC México realiza la primera depuración de nombres que no tenían una resolución correcta o que tuvieran pagos pendientes. Estas acciones permiten darle mayor infraestructura y soporte a la creación de dominios y por tanto páginas con contenidos para nuestro país.

Durante 1998 surge la necesidad de asociarse con otros administradores de códigos territoriales (ccTLDs) para compartir información y discutir políticas de nombres de dominio. Es el 21 de Agosto de 1998 cuando NIC México es cofundador y representante interino de LACTLD, organización que agrupa a los dominios nacionales de Latinoamérica. Asimismo, NIC México organiza en Monterrey la segunda reunión de DNSO, una de las organizaciones de soporte para ICANN, la corporación a cargo de la supervisión de los principales recursos de Internet. El motivo principal es encontrar dominios duplicados y lograr una correcta gestión de los mismos.

En abril de 1999, con el nombre de dominio nestle.com.mx,[423] se inicia la relación entre NIC México y el Instituto Mexicano de la Propiedad Industrial

---

[422] Internet II: el reto, ***Entrevista a Alejandro Pissanty por Ernesto López,*** Reforma, Sección Interfase, México, lunes 13 de julio de 1998, pág 5A.

[423] Al decir de Alejandro Pisanty y Mariana Celorio: "en abril de 1999 el Instituto Mexicano de la Propiedad Industrial (IMPI), le solicitó oficialmente por primera vez a NIC México, la suspensión de un dominio por cuestiones de propiedad industrial; este dominio en controversia fue nestle.com.mx. Más tarde la filial mexicana de Nestlé recobró su legítimo derecho a usar su nombre en Internet. Después de la transferencia de titularidad del dominio nestle.com.mx, NIC

(IMPI) para resolver disputas de nombre de dominio por cuestiones de propiedad intelectual. Posteriormente se definieron mecanismos formales para resolver estos casos. Para mediados de este año son más de 20,000 los dominios registrados bajo .mx.

En septiembre de 1999 entran en vigor nuevas políticas generales, las cuales contienen un procedimiento de resolución de disputas. Este procedimiento tuvo como objetivo resolver los casos más simples de disputas entre marcas registradas y nombres de dominio. De manera exitosa se resolvieron casi 60 casos en 15 meses.

En enero del 2000 había más de 30,000 dominios registrados. Para diciembre de este año hay nuevas políticas y un nuevo procedimiento de resolución de disputas, el cual ahora es administrado por la Organización Mundial de la propiedad Intelectual (OMPI), este procedimiento esta basado en el "*Uniform Dispute Resolution Policy*" (UDRP)[424] el cual es el mismo mecanismo de resolución de disputas utilizados en los dominios genéricos en todo el mundo. OMPI reconoce a NIC México por la implementación de esta política.

Durante el verano del 2001 se establece el Comité Consultivo Externo de NIC México con el objetivo de ser un órgano de consulta, orientado a discutir temas estratégicos y de política para emitir recomendaciones al NIC que coadyuven a alcanzar sus objetivos, con la intención de apoyar el fortalecimiento de NIC-México, así como de impulsar el desarrollo de Internet en México.

Para el 2002 ya hay 75,000 dominios registrados en el .mx siendo el com.mx quien contiene casi el 93% de los registros.

A principios del 2003, con la recomendación positiva del Comité Consultivo, se publican nuevas políticas que entre otras cosas permiten que el nombre de dominio se registre inmediatamente sin intervención humana, se promueve la libertad del registrante de elegir el nombre de dominio que considere apropiado sin revisión de NIC México. Así mismo se redefine la política de solución de controversias, conocida como LDRP.

7.- Internet en México hoy.

El crecimiento del uso de Internet en México está siendo rápido y abrumador; las cifras demuestran crecimientos del 100% en relación al número de usuarios

---

México elaboró el Procedimiento Interno para Resolver Controversias. En los siguientes 15 meses solucionó 55 controversias, de las cuales el 90% se transfirieron a su legítimo titular, algunas de éstas fueron: banorte.com.mx, pepsi.com.mx, danone.com.mx, nivea.com.mx, pedigri.com.mx, texaco.com.mx, hp.com.mx, mtv.com.mx, ado.com.mx, bmw.com.mx, sony.com.mx, pokemon.com.mx, auchan.com.mx. Una controversia que no se resolvió a favor del demandante fue recorcholis.com.mx. El titular del dominio, aunque se trataba de una empresa pequeña con locales de videojuegos, contra otra de grandes vuelos, pudo demostrar su legítima propiedad del dominio. caso yahoo.com.mx tuvo diversas complicaciones pero finalmente el titular del dominio no presentó la información requerida y se transfirió a Yahoo." PISANTY, Alejandro y CELORIO, Mariana, ***.MX, Domicilio conocido en Internet***, Revista Entérate en línea, DGSCA, UNAM, México, Mayo de 2002, http://www.enterate.unam.mx/Articulos/2002/mayo/mx.htm

[424] El sitio de NIC México, existe de forma detallada la ***"Política de solución de controversias en materia de nombres de dominio para .MX"*** y su reglamento, texto completo en: http://www.nic.mx/es/Politicas?CATEGORY=INDICE

y al número de dominios bajo .mx, lo que significa que el fenómeno no ha sido momentáneo sino que se ha convertido en una necesidad el acceso a la información. Para ilustrarnos en la materia es necesario estudiar algunas estadísticas existentes en materia de Internet.

En nuestro país se dio un acelerado crecimiento de los ISP´s. Así notamos que existen hoy en día por ser conservadores actuando en nuestro país más de 50 que actúan en toda la República y que tienen diferentes cantidades de albergue de páginas es decir *hosting*, cifras de la NIC México que nos ilustran los ISP´s con mayor número de dominios en sus equipos bajo .mx.[425]

En cuanto al número de internautas, la Comisión Federal de Telecomunicaciones señala una cifra cercana al millón de usuarios en 1997, pero la cifra en 2006 hablaba de cerca de 19 millones de usuarios.[426]

Otro dato interesante es el porcentaje de dominios bajo .mx y su distribución en relación a la clasificación según la ISO 3166, .mx es decir *hosts* mexicanos, los .com.mx, los relacionados a negocios y comercio en México, los org.mx que se refieren a organizaciones no gubernamentales en el país, los gob.mx que son páginas del gobierno mexicano, ya sea estatal o federal, los dominios edu.mx referentes a los centros educativos en México y por último los net.mx que se relacionan con redes locales de area o LAN, la estadística de distribución de dominios proporcionada por el NIC México,[427] nos señala como la cantidad en función a los dominios .com.mx domina con el 91%. En el mismo sentido los datos más recientes de fecha 14 de marzo de 2007 nos dicen haciendo un comparativo a de su situación en 1997 donde había 177 y en 2007 existen 172 dominios bajo .mx, 441 existían en 1997 en relación a edu.mx, en este año encontramos 4,111, 14,684 bajo el dominio .com.mx en el 97, a diez años de distancia las cifras nos dicen que existen 177,640, es decir unas doce veces más de los que había en la década pasada, los .net.mx eran 482 han disminuido a 465, los .org.mx eran 818 y hoy día son 9,119 por último las páginas gubernamentales bajo .gob.mx eran 383 ahora son 3,663.[428]

---

[425]Ver **Grafico 3** del Apéndice.

[426]A partir del 2001, el Instituto Nacional de Estadística, Geografía e Informática (**INEGI**) genera información estadística sobre la disponibilidad y los usos de las tecnologías de información y comunicaciones en los hogares del país, en particular la cantidad de usuarios de Internet.
La metodología utilizada está basada en una encuesta probabilística en los hogares para recabar datos sobre el acceso y los usos de estas tecnologías. En ella, se define a un usuario de Internet como un residente de seis o más años de edad que accedió, durante los últimos 12 meses, a alguno de los servicios que ofrece esta red.
La información disponible a partir de las encuestas ofrece la oportunidad de presentar datos de los usuarios de Internet desde dos enfoques: a) por lugar donde acceden a Internet y b) por disponibilidad de computadora en el hogar. Asimismo, es posible presentar los cruces de información resultantes de ambos enfoques y enriquecer con ello la perspectiva analítica del tema. En el cuadro del **Gráfico 4** del Apéndice, se presentan ambos enfoques analíticos y sus cruces, a su vez esta la anterior estadística que era proporcionada por la Comisión Federal de Telecomunicaciones, en el siguiente gráfico.

[427]Ver **Gráfico 5** del Apéndice.

[428]Información del ***Network Information Center-México,*** siendo un total de 195,170 en el 2007 contra 16,985 dominios de 1997, la información la podemos encontrar en la dirección electrónica: www.nic.mx/es/Estadisticas.Dominio?type=0 , es interesante señalar que algunos dominios en lugar de crecer disminuyeron como fue el caso de los .mx y los .net, que no tuvieron éxito en nuestro país. Ver **Grafico 5** del Apéndice.

El 80% del millón de personas que al término de 1998 utilizaron Internet en México eran varones, el otro 20% eran mujeres con una tendencia hacia el año 2002 de equilibrar el porcentaje de uso masculino de los servicios de la Red en el país, de acuerdo a las estimaciones que en su momento proyectaba Select-IDC, [429] para abril del 2006 esta situación estaba más que equilibrada según el INEGI, ya que del total de usuarios (18,746,353 mayores de 6 años) 50.6% son hombres y un 49.4% son mujeres, esta misma tendencia se ha dado a partir de 2001, donde el 54.6% eran varones y el 45.4% eran mujeres, vemos entonces que la red ya dejo de ser masculina.[430] Del total de usuarios de Internet en 1998, el 40% se encontraba en las edades de 16 a 25 años, hoy en día según el INEGI el porcentaje es de 26.2%, también en 1998 el 35% entre los 26 y los 35 hoy día ese porcentaje ha disminuido a 18.2% y finalmente 5% en el 98 fluctuaba entre los 36 y 45 años en el 2006 ese porcentaje es de 9.9%.[431]

XI.- Conclusiones

Internet ha cambiado en sus dos décadas de existencia. Fue concebida en la era del tiempo compartido y ha sobrevivido en la era de los ordenadores personales, cliente-servidor, y los *network-computer*. Se ideó antes de que existieran las LAN, pero ha acomodado tanto a esa tecnología como a ATM y la conmutación de tramas. Ha dado soporte a un buen número de funciones desde compartir ficheros, y el acceso remoto, hasta compartir recursos y colaboración, pasando por el correo electrónico y, recientemente, el World Wide Web y la Web 2.0. Pero, lo que es más importante, la red de redes, comenzó como una creación de un pequeño grupo de investigadores y ha crecido hasta convertirse en un éxito comercial con miles de millones de dólares anuales en inversiones.

No se puede concluir diciendo que Internet ha acabado su proceso de cambio. Aunque es una red por su propia denominación y por su dispersión geográfica, su origen está en los ordenadores, no en la industria de la telefonía o la televisión. Puede -o mejor, debe- continuar cambiando y evolucionando a la velocidad de la industria del ordenador si quiere mantenerse como un elemento relevante. Ahora está cambiando para proveer nuevos servicios como el transporte en tiempo real con vistas a soportar, por ejemplo, audio y vídeo. La disponibilidad de redes penetrantes y omnipresentes, como Internet, junto con la disponibilidad de potencia de cálculo y comunicaciones asequibles en máquinas como los ordenadores portátiles y los teléfonos celulares, está posibilitando un nuevo paradigma de informática y comunicaciones "nómadas".

---

[429]Select-IDC es representante exclusivo de ***International Data Corporation (IDC)***, líder mundial en proveer información de mercado, análisis de la industria, y plancación estratégica a usuarios de las Tecnologías de la Información. Select-IDC México analiza el mercado de las tecnologías de la información desde 1989 y el mercado de las telecomunicaciones desde 1995, a través de servicios de información con usuarios y operadores de redes en México. El reporta al que hacemos referencia se intitula: ***El hogar será punta de lanza en el desarrollo de Internet.*** Ubicado en la dirección electrónica: www. select-idc.com.mx/bolpren/internet.htm.

[430] Instituto Nacional de Estadística e Informática, ***Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares,*** Usuarios de Internet por genero, 2001 a 2006. http://www.inegi.gob.mx/est/contenidos/espanol/rutinas/ept.asp?t=tinf216&c=5565

[431]Ver: López, Ernesto, ***Todavía es muy masculina,*** Diario Reforma, Suplemento especial Internet en la Vida Cotidiana, México, Noviembre 12 de 1998, pág.10.

Esta evolución nos traerá una nueva aplicación: telefonía Internet y, puede que poco después, televisión por Internet; está permitiendo formas más sofisticadas de recolección de datos y su probable comercialización. Está cambiando para acomodar una nueva generación de tecnologías de red con distintas características y requisitos: desde ancho de banda doméstico a satélites. Y nuevos modos de acceso y nuevas formas de servicio que dará lugar a nuevas aplicaciones, que, a su vez, harán evolucionar a la propia red y a la legislación en materia de telecomunicaciones, en específico una que regule la protección de datos personales.

La cuestión más importante sobre el futuro de Internet no es cómo cambiará la tecnología, sino cómo se gestionará esa evolución. En este capítulo se ha contado cómo un grupo de diseñadores dirigió la arquitectura de Internet y cómo la naturaleza de ese grupo varió a medida que creció el número de partes interesadas. Con el éxito de Internet ha llegado una proliferación de inversionistas que tienen intereses tanto económicos como intelectuales en la red. Se puede ver en los debates sobre el control del espacio de nombres y en la nueva generación de direcciones IP una pugna por encontrar la nueva estructura social que gulará a Internet en el futuro. Será difícil encontrar la forma de esta estructura dado el gran número de intereses que concurren en la red. Al mismo tiempo, la industria busca la forma de movilizar y aplicar las enormes inversiones necesarias para el crecimiento futuro, por ejemplo para mejorar el acceso del sector residencial. Si Internet sufre un tropiezo en nuestro país, no será debido a la falta de tecnología, visión o motivación. Será debido a que no podemos hallar la dirección justa vía la ordenación jurídica de todos los fenómenos que la red nos plantea; será por la falta de visión de los legisladores mexicanos en encontrar los caminos correctos para gestionar un correcto crecimiento de una tecnología que es la historia de nuestro presente.

CAPÍTULO QUINTO

DE LAS DISTINTAS MANERAS DE ATENTAR CONTRA LA VIDA PRIVADA DE LAS PERSONAS A TRAVÉS DE INTERNET

"Por favor, ¿podrías decirme que camino debería tomar? – preguntó Alicia
Eso depende en gran parte del problema de saber a donde quieres ir – dijo el gato
No me importa mucho a donde iré – dijo Alicia
Entonces no importa mucho que camino tomas – dijo el gato"
Lewis Caroll
Alicia en el país de las maravillas.

CAPÍTULO QUINTO. DE LAS DISTINTAS MANERAS DE ATENTAR CONTRA LA VIDA PRIVADA DE LAS PERSONAS A TRAVÉS DE INTERNET

Mark Lemley, destacado jurista norteamericano y catedrático de la Universidad de Stanford, California, no se equivocaba al argumentar en su obra *Software and Internet Law* que "la historia de la tecnología es también la historia de la invasión de la vida privada"[432]. 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"[433]. De hecho, nadie puede tener certeza de la identidad de la persona o institución que está al otro lado de la computadora 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.

---

[432] LEMLEY, Mark, ***Software and Internet Law,*** Aspen Publishers New York, NY, 2003, pág. 111.
[433] PÉREZ LUÑO, Antonio, ***Dilemas actuales de la protección de la intimidad.*** Revista Ius et Praxis Universidad de Lima. Perú, 1992, Nº 21-22. pág. 13.

I.- 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 ordenamientos jurídicos, como lo estudiamos con anterioridad. Con la llegada de Internet, se ha popularizado una nueva alternativa de correspondencia alrededor del planeta: el llamado correo electrónico, o *email* (*electronic mail*) estudiado también con anterioridad.

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 una computadora a otra. 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 Estado Unidos más de 135 millones de personas tendrían una cuenta de correo electrónico, y se calcula que circulan diariamente por la red acerca de 500 millones de mensajes enviados (sólo en Norteamérica).[434] Según un reportaje de fecha 15 de mayo de 2006 del diario Reforma mexicano, circularían cerca de 60 mil millones de *emails* al día, y es un hecho que esta cifra aumenta cada día.[435]

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 *email* 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, etcétera. Tratándose de mensaje enviados a través del correo electrónico, no existe garantía 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.

---

[434] GOOD, Edgar, ***An email Education. What You D'ont Know About Email Can and Will Hurt You***, International Journal of Communications Law and Policy, Oxford University, U.K. 1999, pág. 12.

[435] El 15 de mayo de 2006, el diario nacional Reforma publicó un artículo titulado "Correo electrónico y abuso". Donde su autor cita la siguiente dato: "Según cifras proporcionadas por el Jefe Ejecutivo de *Deutsche Telecom*, Kai-Uwe Ricke, cada día son enviados 60 mil millones de correos electrónicos a través de Internet lo que, unido a la sofisticación cada vez mayor de los delitos cometidos por esta vía, significa un gran peligro para todos los usuarios " . LÓPEZ, Eduardo, ***Correo electrónico y abuso***, Sección Interfase, Diario Reforma, México, 15 de mayo de 2006.

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 *email* es ubicuo,[436] ya que no tiene un destino físicamente determinado, sino que puede ser recogido a través de cualquier computadora que se encuentre conectada 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*[437] que provee de este servicio a los usuarios, independientemente donde éstos se encuentren. Esta página de acceso permite que el titular 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 Giraldo 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".[438] Incluso, la propia página de acceso a la cuneta de correo electrónico ofrece servicios en caso de que la clave de acceso haya ido olvidada. El correo tradicional funciona a través de un servicio postal bastante distinto.

Hechas las distinciones pertinentes, podemos entrar a dar una definición más concreta de correo electrónico, *email* o *electronic mail* diferente a la ya estudiada en el capítulo anterior: "aplicación mediante al cual un ordenador puede intercambiar mensaje 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".[439]

De lo anteriormente explicado se puede también determinar las características del correo electrónico[440]

---

[436] El Diccionario de la Real Academia de la Lengua Española entiende por ubicuo: "qué está presente en un mismo tiempo en todas partes". Vigésima segunda edición, www.rae.es Esto aplicado al correo electrónico tiene implicaciones tecnológicas que implican que el mismo puede ser consultado, en cualquier parte donde exista una conexión a Internet, una Red Inalámbrica o algún tipo de dispositivo que nos permita acceder a una página *web* o *wap* que tenga disponible el servicio. Así incluso podemos consultar nuestro *email* en el teléfono celular.

[437] Para mayor información sobre correo electrónico, se recomienda consultar el apartado V, del Capítulo Cuarto, en su numeral 3, intitulado Correo Electrónico (*electronic mail, email*)

[438] GIRALDO QUINTERO, Argiro, ***El Secreto en la Comunicación por Correo Electrónico***, Revista Electrónica de Derecho Informático, Número 025, agosto del 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=539

[439] FERNANDEZ CALVO, Rafael, ***Glosario básico inglés-español para usuarios de Internet***, Asociación de Técnicos de Informática, http://www.ati.es/novatica/glosario/glosario_internet.html

[440] Para ver con más detalle estos puntos, remitirse a GERALDO QUINTERO, Argiro, ***El Secreto en la Comunicación por Correo Electrónico***, Revista Electrónica de Derecho Informático, Número 025, agosto del 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=539

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 enlutar el mensaje.

La cuenta de correo electrónico, desde mi punto de vista, debe ser considerada como un dato de carácter personal y tener la protección de los datos considerados como tales, en los países donde este legislado. Esta protección ya ha sido reconocida, como lo señala Paloma Llaneza González, por el Consejo Europeo, que afirma que "la dirección de correo electrónico es un dato personal".[441] 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 y que se debe de reconocer en nuestro país.

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 ente ilícito procurando que no pase como tal. Entidades que prestan el servicio de correo electrónico como Hotmail o Yahoo![442]reconocen que debe existir secreto en cuanto al contenido y uso que cada persona 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

---

[441] LLANEZA GONZÁLEZ, Paloma, ***Internet y Comunicaciones Digitales***, Editorial Bosch, Barcelona, España 2000, pág. 271.

[442] Según lo señala el colombiano GERARLDO QUENTERO, Argiro "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 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 transmisión, pero éste y sus representantes estarán facultados (pero 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 Contenido que vulnere las Condiciones o que de algún modo sea inaceptable" ***El Secreto en la Comunicación por Correo Electrónico***, Revista Electrónica de Derecho Informático, Número 025, agosto del 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=539

funcionamiento del sistema. Las palabras del norteamericano Barry Fraser ilustran estos 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.[443] Adicionalmente, el mensaje puede ser interceptado si el remitente o el destinatario del mensaje consienten. 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".[444] Profundizando en las consecuencias de lo que esto puede traer, muchos han puesto en tela se 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.[445]

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. [446]

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 le que sucedió con fecha 2 de abril 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."[447]

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.

---

[443] En el capítulo segundo se estudia la ECPA de forma amplia.

[444] FRASER, Barry, ***Rules of the Road Navigating the Information Superhighway***, Human Rights Magazine, Volume 26, No 1, 1999. http://www.abanet.org/irr/hr/winter99_fraser.html

[445] Al respecto, POMEROY, Jeremy en ***Online Anonymity can be Illusory Under Current Law, ISP Policies*** Multimedia & Web Strategist, Sept. 1998, pág.6, 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 transforma 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 parte."

[446] En nota publicada por CNN *online*, se relata que 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. ***New Hotmail breach reported***, 14 de septiembre de 1999, http://www.cnn.com/TECH/computing/9909/14/hotmail/index.html

[447] ***Los socialistas franceses denuncian un correo falso en su nombre***, Nota publicada en http://delitosinformaticos.com/noticias/101761230840490.shtml, visitado en abril del 2002.

Muchas propuestas en torno a cómo afrontar este problema han surgido por todo el mundo y de todos los tipos. Hay quienes ven una solución en la creación de un "organismo multinacional"[448], otros creen que la solución está en manos de los proveedores del servicio de Internet, más precisamente los operadores del sistema a cargo de 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.[449]

Otros, como la prestigiada abogada ecuatoriana María 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.

II.- 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 auge. Surgieron quienes se dedicaban a enviar diariamente publicidad a través del fax, o quienes a través de grabadoras llamadas 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 promulgación 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.[450]

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

---

[448] GERALDO QUINTERO, Argino 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 intimidad, 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 vulnerable por la criminalidad globalizada no puede acabar con las conquistas humanas en materia de derechos fundamentales." ***El Secreto en la Comunicación por Correo Electrónico***, Revista de Derecho Informático, Número 025, agosto del 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=539

[449] BARRERA María Helena, se refiere a los inconvenientes de esta solución en el sentido de que: "Los problemas que conlleve 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 más vasto y global. En segundo legal, 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***, Revista de Derecho Informático, No.015, octubre de 1999, http://www.alfa-redi.org/rdi-articulo.shtml?x=345

[450] Ver, más sobre la *Telephone Consumer Protection Act* en texto de LEÓN LEÓN, Carlos Alfredo en ***Consideraciones Legales Relativas al Envío de emails. Comerciales No Solicitados***, dicho texto publicado en Revista de Derecho Informático, Número 036, julio de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=730

tienen una cuenta de correo electrónico recibir con muchísima frecuencia correo no solicitados o "correo basura" (*junk mail*).

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* 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 cadena (*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".[451] Desde un punto de vista más general, otros, lo han definido de la siguiente manera: "correo basura que por lo general no tiene carácter comercial, pero si es una "baratija" (la traducción literal de *junk* es baratija), es decir son mensajes que llenan el buzón incomodándolo."[452]

Cuando en el año 2000 escribí sobre el *junk mail* en específico señale: "¿de que modo estos mensajes afectan la intimidad personal? ¿La vulneran o la violentan? Es claro que para poder recibir estos mensajes uno tiene que ser parte de una lista de direcciones electrónicas que aparecen en el *header* (cabecera) del mensaje. En los casos de usuarios más avanzados que utilizan estas herramientas, procuran colocar a los usuarios en bcc (*blind carbon copy*) de modo tal que no aparecen todas las direcciones a las cuales se ha enviado dicho "*junk mail*", mas esto es considerado una falta a las *nettiquets* y además una violación clara del espacio de la intimidad, pues en la mayoría de los casos estos mensajes no tienen más función que "llenar el buzón de correo".[453] Quitan tiempo." De esto puedo obtener la diferencia clara entre *spam* y *junk*, el primero tiene fines comerciales y el segundo no necesariamente tienen que serlo, ya que pueden ser correos con bromas, *chain letters* o *hoax*[454], pero a final de cuentas violentan nuestro espacio de privacidad.

El llamado *spam* o bombardeo publicitario se define tradicionalmente como "los mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico".[455] Se trataría

---

[451] LLANEZA GONZÁLEZ , Paloma, ***Internet y Comunicaciones Digitales***, Editorial Bosch, Barcelona, España, pág. 271

[452] FERREYRA, Gonzalo C, ***Internet paso a paso: Hacia la autopista de la información***, Grupo Editor Alfaomega, México, 1996, pág. 35.

[453] JIMÉNEZ GUZMÁN, Luis, ***Hacia una regulación del comercio electrónico en México***, Tesis Profesional, México, 1999, pág. 161.

[454] Un ***hoax*** (del inglés: engaño, burla) es un intento de hacer creer a un grupo de personas que algo falso es real. En el idioma español el término se popularizó principalmente al referirse a engaños masivos por medios electrónicos especialmente Internet. A diferencia del fraude el cual tiene usualmente una o unas cuantas víctimas y es cometido con propósitos delictivos y de lucro ilícito, el *hoax* tiene como objetivo el ser divulgado de manera masiva haciendo uso de los medios de comunicación, siendo el más popular de ellos en la actualidad Internet y no suelen tener fines lucrativos o no son su fin primario. Las personas que crean *hoaxes* tienen diversas motivaciones dentro de las que se encuentran el satisfacer la vanidad personal, la intención de hacer una broma para avergonzar o señalar a alguien o la pretensión de provocar un cambio social haciendo que la gente se sienta prevenida frente a algo o alguien, también suele ser característico dentro de los autores de *hoax* el querer mofarse y hacer evidente la credulidad de las personas y de los medios de comunicación. ***Wikipedia. La enciclopedia libre***, http://es.wikipedia.org/wiki/Hoax . Ver ejemplos en Anexo 3 del apéndice esta obra.

[455] Esta definición es la obtenida en ***Wikipedia. La enciclopedia libre***, dentro de esta voz, encontramos un interesánte dato sobre el origen de la palabra *spam*: "Tiene raíces estadounidenses con unas curiosas derivaciones socio-culturales: La empresa chacinera estadounidense *Hormel Foods* lanzó en 1937 una carne en lata originalmente

en este caso de publicidad que tiene intenciones comerciales. Según un estudio del *New York Times* 9 de cada 10 mensajes que se mandan a través de Internet constituyen correos electrónicos no deseados.[456]

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 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. [457] Esto se traduciría por ejemplo en el tiempo en que uno se demora en leer y eliminar estos correos. Desde otra perspectiva, muchas 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 un dato personal, ha sido revelado sin su conocimiento.

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

---

llamada *Hormel's Spiced Ham*. El gran éxito del invento lo convirtió con el tiempo en una marca genérica, tan conocida que hasta el mismo fabricante le recortó el nombre, dejándolo con solo cuatro letras: *Spam*. El *Spam* alimentó a los soldados soviéticos y británicos en la Segunda Guerra Mundial, y desde 1957 fue comercializado en todo el mundo. En los años 60 se hizo aun más popular gracias a su innovadora anilla de apertura automática, que ahorraba al consumidor el uso del abrelatas. Fue entonces cuando los *Monty Python* (grupo de comediantes ingleses) empezaron a hacer burla de la carne en lata. Su divertidísima costumbre de gritar la palabra *spam* en diversos tonos y volúmenes se trasladó metafóricamente al correo electrónico no solicitado, que perturba la comunicación normal en Internet. En un famoso *sketch* de 1970 (*Flying Circus*) los comediantes británicos representaban a un grupo de hambrientos vikingos atendidos por solícitas camareras que les ofrecían "huevo y panceta; huevo, salchichas y panceta; huevo y *spam*; huevo, panceta, salchichas *y spam; spam*, panceta, salchichas y *spam; spam*, huevo, *spam, spam*, panceta y *spam*; salchichas, *spam, spam*, panceta, *spam*, tomate y *spam*, ...". La escena acababa con los vikingos cantando a coro "*Spam, spam, spam, spam*. ¡Rico *spam*! ¡Maravilloso *spam*! *Spam, spa-a-a-a-a-am, spa-a-a-a-a-a-am, spam*. ¡Rico *spam*! ¡Rico *spam*! ¡Rico *spam*! ¡Rico *spam*! *Spam, spam, spam, spam*!". Como la canción, el *spam* es una repetición sin fin de texto de muy poco valor o ninguno, que aplicado a los mensajes electrónicos, se refiere a los mensajes enviados de forma masiva y dirigidos a personas que, en principio, no desean recibirlos. http://es.wikipedia.org/wiki/Spam

[456] STONE, Brad, **Spam *Doubles, Finding New Ways to Deliver Itself*** Según traducción textual: "En los últimos seis meses, el problema ha empeorado radicalmente. La cantidad de *spam* generado en todo el mundo se ha doblado desde el último año, de acuerdo con *Ironport*, una firma dedicada al filtrado de *spam*, y el correo basura alcanza ahora una proporción de 9 de cada 10 mensajes de *email* mandados por Internet" *New York Times*, 6 de diciembre de 2006.

[457] Citado por ROBERTO SOBRINO, Waldo Augusto, ***Las "Cookies" y el "Spam" (y la violación de la "Privacidad" y la "Intimidad")***.Revista de Derecho Informático No.035 de junio de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=710

las personas que reciben esta correspondencia. Es casi seguro que aquella base de datos no cumpla con los requisitos que establecen leyes europeas, latinoamericanas o norteamericanas como las ya estudiadas en el capítulo segundo, y por consiguiente se trate de bases 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."*, tramitida en la Corte de Pennsylvania, de fecha 4 de Noviembre de 1996, donde entre varias interesantes cuestiones, la empresa acusada de "*spam*", basada su defensa en al "Primera Enmienda" ("*freedom speech rights*"), e incluso se analizó la legalidad de "*America Online*" de enviar "*email bombs*"".[458] Como consecuencia de ello, se originó en el Congreso Norteamericano un proyecto de ley, la *Unsolicited Electronic Mail Act* del 2000 (H.R. 3113), durante esa legislatura (la 106) existieron 11 proyectos para regular el *spam*, de la legislatura 107 a la 109 existieron 20 proyectos de los cuales solo uno fue aprobado.[459] La iniciativa en comento señala que: "Este proyecto establece que en un *email* comercial no solicitado que se encuentre marcado o rotulado como tal, se deben incluir 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 *mails* utilizando sus servicios".[460] Cabe señalar que en el 2003 se aprobó por el Congreso Norteamericano la *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*, también conocida como CAN-*SPAM Act of 2003*[461] y más recientemente el 22 de diciembre de 2006 la *US Safe Web Act of 2006.*[462] Sin embargo, la promulgación de cualquier norma referente a Internet debe considerar el problema de la aterritorialidad de la red, ya que como veíamos anteriormente, la aplicación de una ley 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

---

[458] Ibídem, refiriéndose a información obtenida en *Electronic Commerce & Law Report*, de fecha 1 de Diciembre de 1997.

[459] Información abundante sobre estos proyectos se encuentra en la página de ***Spam Laws***, en www.spamlaws.com

[460] La información sobre este proyecto fue obtenida en la Librería del Congreso Norteamericano, ***The Library of Congress. Thomas***, http://thomas.loc.gov/cgi-bin/query/z?c106:H.R.3113:

[461] Para mayor información ver FILHO, Democrito. R, ***Short commentaries on the CAN-SPAM Act***, Revista de Derecho Informático, No. 70, mayo del 2004, http://www.alfa-redi.org/rdi-articulo.shtml?x=1093

[462] Busca proteger a los consumidores frente al correo basura, el *software* espía y el fraude a través de Internet, permitiendo a la Comisión Federal de Comercio compartir información e investigar conjuntamente con sus interlocutores en otros países. La nueva Ley autoriza a la Comisión Federal de Comercio a proporcionar ayuda para la investigación a instituciones extranjeras que sean competentes para reprimir prácticas comerciales fraudulentas o engañosas, incluyendo la posibilidad de intercambiar temporalmente personal para colaborar en tales actuaciones. A estos efectos, la Comisión podrá negociar con sus contrapartes de otros países los acuerdos que formalicen la provisión de ayuda, materiales o información.

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 al *Telephone Consumer Protection Act*) como en Europa.[463] Al decir de Pedro Alberto de Miguel Ascencio,[464] el debate en la Unión Europea entre un régimen de listas de inclusión o de exclusión fue resuelto por el artículo 13 de la Directiva 2002/58/CE, sobre la privacidad y las comunicaciones electrónicas, que entendió con ciertas matizaciones a los mensajes de correo electrónico el restrictivo régimen previsto par el fax y los sistemas automáticos de llamada. El concepto de correo electrónico que no requiere la participación simultanea del remitente y del destinatario, como es el caso entre otros, de los mensajes SMS, MMS y de los mensajes dejados en contestadores automáticos. 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 solicitado. 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 embargo, 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. 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.

La situación en nuestro país al decir de la doctrina existente,[465] es la de contar con un sistema de listas de exclusión (*opt-out*) según lo señala el artículo 18 de la Ley Federal de Protección al Consumidor, que se refiere a que la Procuraduría Federal de Protección al Consumidor pueda llevar un registro público que será gratuito, de consumidores que no deseen que su información sea utilizada con fines publicitarios, quienes podrían comunicar a la PROFECO

---

[463] Para apuntalar el comentario es importante señalar que el día 7 de diciembre de 2001, se publicó la siguiente noticia en el sitio de Internet Vlex en su sección Actualidad: ***Los quince adoptan la opción* opt-in *dentro de la propuesta de la Directiva sobre el* spam,** "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 *'optin'*. 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 de Telecomunicaciones en los Quince sirvió, además para la presentación por la Comisión del Séptimo Informe sobre la Implementación del paquete Legislativo sobre Telecomunicaciones, para la adaptación 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 *'optin'* 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 a través 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." http://premium.vlex.com/actualidad/Actualidad-vLex/Los-Quince-adoptan-opcion-%27opt-in%27-dentro-propuesta-Directiva-%27spam%27/2100-118803,busqueda_3613951,01.html

[464] DE MIGUEL ASENCIO, Pedro Alberto, ***Derecho del Comercio Electrónico***, Editorial Porrúa, México, 2005, pág. 213.

[465] Ver a RAMIREZ CHELALA, Yesín y VERA PRENDES, Luis o a DE MIGUEL ASENSIO, Pedro Alberto.

su solicitud de inscripción en este registro, además el artículo 18 bis del mismo ordenamiento prohíbe a los proveedores y empresas el envió de publicidad a los consumidores que expresamente les hayan manifestado su voluntad de no recibirla o que estén inscritos en el registro del artículo 18. Cabe destacar que antes de la reforma de 2004 se fijo la precisión de los artículos mencionados ya que con anterioridad sólo contaba con el artículo 76 bis cuya fracción VI se limita a establecer que el proveedor debe respetar la decisión del consumidor de no recibir avisos comerciales, pero sin incluir reglas específicas sobre el envió de mensajes de correo electrónico ni disposiciones sobre la puesta a disposición de los consumidores de vías para manifestar su oposición a la recepción de esos envíos. Así con la reforma el artículo 17 quedo como sigue:

> ARTÍCULO 17.- En la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor; de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la Procuraduría.
> *Párrafo reformado DOF 04-02-2004*
> El consumidor podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad. Asimismo, el consumidor podrá exigir en todo momento a proveedores y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial.
> *Párrafo adicionado DOF 04-02-2004*

Se transcribe el numeral porque es importante señalar que se habla por primera vez en una legislación nacional de la dirección electrónica de un proveedor y el segundo párrafo señala que el consumidor puede exigir no ser molestado en su dirección electrónica para que les ofrezcan bienes de consumo, afirmando así la exclusión.

III.- Las *cookies* o galletitas

Se definen tradicionalmente como *cookie* (espía, cukie, caqui, fisgón, galletita) a "los ficheros de datos guardados en un directorio específico del ordenador del usuario. Se crean por los servidores *web* con el objeto de ser enviados a los programas navegadores del usuario, y así recoger la información de que dicho fichero ha reunido. Por lo tanto son considerados como datos personales". [466] Otros han preferido definirlas como "un fragmento de información que se almacena en el disco duro del visitante de una página *web* a través de su navegador, a petición del servidor de la página. Esta información puede ser luego recuperada por el servidor en posteriores visitas. Las inventó Lou Montulli, un antiguo empleado de *Netscape Communications*. Al ser el protocolo HTTP incapaz de mantener información por sí mismo, para que se pueda conservar información entre una página vista y otra (como *login* de usuario,

[466] Definición propia. ***Hacia una regulación del comercio electrónico en México***, Tesis profesional, México 1999, pág.157

preferencias de colores, etc), ésta debe ser almacenada, ya sea en la URL de la página, en el propio servidor, o en una *cookie* en el ordenador del visitante."[467]

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* 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 persistente 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.[468]

Para empezar, lo que se deja el disco duro del usuario es un inofensivo dichero de texto (con extensión ".txt") y no fichero ejecutable (".exe", ".com", ".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 puede determinar la dirección de e-mail o la identidad del usuario los facilitan de una manera voluntaria.

- Un sitio *web* sólo puede recoger las "cookies" que dejó el mismo, es decir, no puede recoger las "cookies" provenientes de otros sitios."[469]

- Para su aplicación, muchos servidores utilizan el sistema *Opt-in*, es decir la instalación de las *cookies*. Sin embargo, no siempre esta política ha sido respetada.

Como señalaba la definición de *Wikipedia*, 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

[467] Definición de ***Wikipedia. La enciclopedia libre***. Mas información sobre el tema en: http://es.wikipedia.org/wiki/Cookie

[468] Esta clasificación se encuentra en la descripción que el servidor 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.

[469] S ELIAS, Miguel, ***Situación Legal de los Datos de Carácter Personal frente a las Nuevas Tecnologías,*** Revista de Derecho Informático, No. 032, marzo de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=638

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* 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 constituye 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 del aquel entonces vicepresidente de Estados Unidos, Al Gore en 1998. De ello se desprendieron los siguientes resultados: de 1400 *websites* comerciales visitados, un 85% recogía y almacenaban datos personales de los visitantes. Sólo un 14% deban algunas indicación acerca de intimidad de la información recogida y sólo un 2% ofrecía una política a favor de los usuarios con sentido.[470]

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 demasiada veces" y que "esta metodología cuestionada les permite suministrar a sus empresas afiliadas, información precisa para que luego estas sugieren correctamente ciertos productos a los clientes". Este caso fue planteado ante la *Federal Trade Comisión* que fue resuelto por la Suprema

---

[470] Información en CASCUBERTA, David, ***La privacidad en los nuevos medios electrónicos. Aspectos éticos y sociales***, Revista de Derecho Informático. No. 011, junio de 1999, http://www.alfa-redi.org/rdi-articulo.shtml?x=276

Corte de los Estados Unidos favorable a *Doubleclick*,[471] así la jurisprudencia norteamericana determino que el uso de *cookies* con fines de publicidad no viola la privacidad ni las normas sobre comunicaciones electrónicas (ECPA), a pesar de lo que la doctrina ha sostenido. Pero en un nuevo litigio contra *Pharmatrack*[472] la Corte revirtió su criterio y determino que si es ilegal y va en contra de la ECPA, el uso de *cookies* con fines de publicidad y recolección de datos apegándose así a lo dicho en la doctrina.

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.[473]

En la actualidad, hay quienes creen que las *cookies* pueden convertirse en un mecanismo que no atenta 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 usuarios se percate, y ello debe considerarse en la actualidad donde la tecnología ha podido más que las buenas intenciones.

IV.- El derecho a la vida privada y los Proveedores del Servicio de Internet (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).[474] 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,

---

[471] In re *Doubleclick Inc. Privacy litigation, 2001 U.S. Dist. LEXIS 3498* (2001). Este criterio fue revertido por un reciente fallo en el caso "Pharmatrack".

[472] In Re *Pharmatrak, Inc. Privacy Litigation*, 329 F 3d 9 (Ist Cir. May 9, 2003)

[473] Al decir de RAMÍREZ RAMÍREZ, Agustín, "toda la información contenida en el expediente clínico se encuadra en el concepto de "datos personales", de tal suerte que las instituciones públicas prestadoras de servicios médicos cuentan, entre sus archivos, con información de los datos de salud –tanto físicos como mentales- de la mayor parte e la población de nuestro país. Lo anterior no pasaría de ser un dato estadísticamente trascendente, si no fuera por las implicaciones que puede tener este criterio en la relación médico-paciente y en la forma de ejercer la medicina pública", nuestra preocupación va más a la parte de las instituciones médicas privadas que no tienen a la fecha algún control sobre esos expedientes que contienen datos personales, porque después de leer lo dicho por Ramírez en la parte pública estamos de una u otra forma cubiertos. RAMÍREZ RAMÍREZ, Agustín, Tratamiento jurídico de los datos clínicos en México (Información y límites de acceso) en CIENFUEGOS SALGADO, David y MACÍAS VÁZQUEZ, María Carmen, ***Estudios en homenaje a Marcia Muñoz de Alba Medrano Bioderecho, tecnología, salud y derecho genómico***, Instituto de Investigaciones Jurídicas, UNAM, México, 2006, pág. 338.

[474] Ver el Capítulo Cuarto de esta obra en su apartado número II.- Internet: Red de redes, el numeral 4.- Los Proveedores de Servicios Internet (*Internet Service Providers*)

hospedaje de página *web*, consultoría de diseño e implantación de *webs* e Internet, etc.,)".[475] Resultan interesantes además mencionar que en nuestra legislación no se habla directamente de Proveedores de Servicio de Internet, pero una interpretación al artículo 3 fracción XII, de la Ley Federal de Telecomunicaciones nos da una idea al señalar que es "servicio que presta un usuario de la red concesionada o red pública de telecomunicaciones, cuya actividad tiene efecto en el formato, contenido, código, protocolo, almacenaje o aspectos similares de la información transmitida".

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 no 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 Laflecha.net, y que literalmente dice que:

> Marqueze garantiza la confidencialidad de sus datos al incorporarlos a un fichero de nivel de seguridad alto, inscrito en la Agencia de Protección de Datos, con la finalidad de gestionar la prestación del servicio y permitir poner en contacto a los usuarios entre sí y a su vez con la empresa Marqueze Telecom, S.A, a través de las distintas plataformas desde las que sea accesible el servicio, tales como Internet, Televisión, prensa o cualquier otro apto para la prestación del servicio, y la remisión por parte de esta compañía, destinataria de los datos, de información sobre productos y servicios, propios o de terceras personas, que pudieran ser de su interés, para lo cual usted presta su consentimiento. Dado que entre sus datos pueden encontrarse algunos especialmente protegidos como los de orientación sexual, se le informa de su derecho a no proporcionar estos datos. Así mismo usted presta el consentimiento para dicho tratamiento.
>
> El usuario presta su consentimiento expreso e inequívoco que para el tratamiento de los datos recogidos con la finalidad prevista en el párrafo anterior se efectúe a través de un servidor ubicado en un datacenter, situado en Madrid, España, mediante Comvive Servidores S.L cuyas prestación del servicio se encuentra en http://www.comvive.es/ [476]

[475] Definición obtenida del glosario de Términos Informáticos en http://www.ati.es/novatica/glosario/glosario_internet.html, visitado en marzo del 2002.
[476] Consultar condiciones de privacidad de www.laflecha.net

Un caso distinto es el de los proveedores 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 responsabilidad de los contenidos injuriosos.[477]

Como un ejemplo, al no existir en nuestro país un solo caso de interpretación judicial en este sentido debemos ilustrar el ocurrido en la jurisprudencia chilena donde existe un caso de similares características al ya narrado 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, etcétera, 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 teléfono privado. Esto dio lugar a desagradables episodios que produjeron, entre otras cosa, 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, sea 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,

[477] La información de este caso fue obtenida del informe de JIJENA LEIVA, Renato en ***Responsabilidad de los ISP por la difusión de contenidos*** **online**, págs. 7 y 8. el mismo autor también se refiere ala 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, argumentado 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". Revista Electrónica de Derecho Informático, No. 15, octubre de 1999, http://premium.vlex.com/doctrina/REDI-Revista-Electronica-Derecho-Informatico/Informe-legal-Improcedencia-censurar-legalmente-contenidos-Internet-Analisis-Boletin-N%B02395-19/2100-107405,01.html

> el proveedor de contenido y los usuarios o destinatarios finales del servicio.
>
> El proveedor de acceso permite que un determinado usuario de conecte con la red Internet, que de no existir ese acceso haría imposible la comisión del ilícito; el proveedor de sitio o almacenamientos,, en la medida que permita que un determinado sitio *web* en el que se cometan actos ilícitos permanezcan almacenados en su 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 redeterminado sitio *web*".[478]

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 www.tribu.grupoweb.cl. La calidad de proveedor de contenido la tiene por su parte la empresa "Grupo web". 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, Santiago Schuster Vergara, la responsabilidad recae directamente en el usuario proveedor de contenido en la red. Puede además extenderse 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 determinan 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,[479] donde la responsabilidad recaería en los ISP

---

[478] Considerando 19° del Recurso de Protección N° 243-1999 contra ENTEL Chile, en el Archivo de Gaceta Jurídica, N° 239, pág. 229, edición de Mayo del 2000. Santiago, Chile.

[479] 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 VALLEPUGA GONZÁLEZ, Paula 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. servicio 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 comunicaciones. Estos servicios de mera transmisión engloban el almacenamiento sirva exclusivamente para ejecutar la 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 daros: consiste en almacenar datos facilitados por el destinatario del servicio. Esta clasificación coinciden con la realizada por el Anteproyecto de Ley de Comercio Electrónico español, que ha sido aprobado el 7 de febrero de 2000. El Anteproyecto los denomina, respectivamente, operadores 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

"cuando puedo pueda esperarse razonablemente que son conscientes de que aquel es *prima facie* ilegal no han tomado medidas razonables para eliminar dicho contenido una vez que el mismo ha traído claramente su atención."[480]

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 IPS son o no responsables por los actos cometidos contra la vida privada de las personas. A ello ha salido al paso la doctrina, 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 posición 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".[481] En lo personal, comparto las posturas antes mencionadas, ya que 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 al 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 esto no se convierta en cuna de delitos cometidos a través del ciberespacio.

La legislación española, a través de la Ley de Servicios de la Información y del Comercio Electrónico, más conocida como LSSICE, regula la presencia de contenidos ilícitos en red, responsabilizando a los ISP en caso de que, al estar

---

servicio no serán responsables, siempre que: (1) n no hayan originado ellos mismos la transmisión; 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 ampliamente reconocida y utilizada por el sector, con el fin de obtener datos sobre la utilización de la información; y n actúe rápidamente efectivo de que: b la información ha sido retirada del lugar de la red en que se encontraba inicialmente; b de que se ha imposibilitado el acceso a ese información; b 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: b no tenga conocimiento de lo dispuesto en el párrafo anterior, el PSI actué 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 circunstancias conocen que una actividad o información es ilícita deberá o bien retirarla, o bien impedir el acceso a la misma." ***Responsabilidad de los Prestadores de Servicio en la Sociedad de la Información***, Revista de Derecho Informático, No. 030, enero de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=615

[480] CARRASCO BLANC, Humberto, ***Algunos Aspectos de la Responsabilidad de los Proveedores de Servicios y Contenidos de Internet. El caso "ENTEL"***, Revista de Derecho Informático, No. 26, septiembre de 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=554

[481] JIJENA LEIVA, Renato, ***Op. cit.***

al tanto de que su servidor posee algún contenido ilícito, no lo hayan comunicado a la Administración.[482] Es así que dicha ley, en su exposición de motivos en el punto tercero segundo párrafo 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 sigan 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".[483]

En todo caso, hay quienes creen que la solución está en que los proveedores de servicio de Internet instalen programa filtro en la red que impida el acceso a sitios *web* ilegales. Otros creen que la solución más factible es la autorregulación, o la firma de Tratados Internacionales que legislen sobre el tema.

V.- ¿Las páginas *web* protegen efectivamente nuestro derecho a la vida privada?

Además 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 atetan muchas veces contra el derecho a la vida privada de las personas sin que siquiera nos percatemos de ello. 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 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 estos, 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,

---

[482] Esta información se obtuvo de una entrevista realizada a la exministra de Ciencia y Tecnología española Anna Birulés, publicada en la revista ***Cuenta y Razón del pensamiento actual***, Entrevista con Anna Birulés, Ministra de Ciencia y Tecnología, No. 117, La Rioja, España, pág. 141-143.

[483] Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, o LSSICE, punto tercero, párrafo segundo de la exposición de motivos. 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. Se puede visitar en la página: "La ley de Internet fácil" del Ministerio de Industria, Turismo y Comercio de España: http://www.lssi.es/Secciones/Normativa/

valiosa información, a un directorio público en Internet.[484] 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.[485]

En nuestro país los casos más importantes fueron en el sector público. En mayo de 2003 se puso al descubierto que la empresa *Choice Point* vendió al gobierno de Estados Unidos bases de datos de uso privativo del Estado mexicano desde 18 meses atrás, las investigaciones permitieron conocer que en 2001, la empresa Soluciones Mercadológicas en Bases de Datos vendió en 335 mil dólares a *Choice Point* la base de datos del padrón electoral del Instituto Federal Electoral, en el que se incluía información de 58 millones de votantes mexicanos.[486]

Así mismo, la *American Civil Liberties Union* (ACLU) habría solicitado en junio de 2002 a la *Federal Trade Comisión* (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.[487]

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, CURP, IFE, cédula profesional, estado civil, etcétera. A pesar de que este tipo de páginas no es muy popular en México, en Europa y Estados Unidos son una práctica frecuente. He querido presentar un caso concreto con las siguientes páginas de Internet que prestan sus servicios en Argentina y Estados Unidos respectivamente. 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, así como otros datos sensibles. 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 da *click* en los mismos. La segunda, como se lee en ella, revela por una suma de dinero, información "demasiado" completa sobre nuestra vida personal.[488]

Como consecuencia de la indiscriminada transferencia de datos de carácter personal que se efectúan a través de Internet, ya algunos ordenamientos

---

[484] Información publicada en el diario español "El País" ***Passport almacena los datos de 150 millones de usuarios***, 25 de octubre de 2000.

[485] Información publicada en el diario español "Elmundo.es" ***La agencia de protección de datos multa a Terra***, 28 de marzo de 2001.

[486] Información obtenida del diario "El Universal", ***Multa millonaria a vendedores del padrón electoral***, en su edición del día, sábado 16 de diciembre de 2006. http://www.eluniversal.com.mx/notas/394453.html

[487] Esta noticia se publico en la página *web* de Newsbytes.com, para ver más detalle de esta información, remitirse a http://www.newsbytes.com

[488] Ver Anexo 2 del apéndice de esta obra.

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 alcanzando 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 grandes 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 le derecho a la intimidad y la protección de la seguridad. Esta 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 lo últimos puntos de fricción de la propuesta original, en especial, el referido al correo electrónico publicitario con fines de venta, que, como general, no podrá ser enviado sin autorización previa del receptor.[489]

A nivel América Latina, 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.

VI.- Internet como medio de control de 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

[489] Esta noticia puede leerse con detalle en artículo publicado por el diario español "Edmundo.es" de fecha 7 de diciembre de 2001, ***"Decisión de los ministros de telecomunicaciones. La UE respetará la privacidad de datos en Internet salvo cuando afecten a la seguridad"***, para acceder directamente a este artículo, remitirse a http://www.elmundo.es/navegante/2001/12/07/seguridad/1007715325.html

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 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 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 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 e incluso sensibles, y que pueden amenazar la vida privada del postulante, como por ejemplo su tendencia política, su religión, 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.[490]

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 privacidad 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?[491]

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 Jiménez Román, el empleado despedido, tuvo sus fundamentos en que se violó su correspondencia y por consiguiente se atentó contra su vida privada 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 mensaje a través de Internet, muchos de ellos con contenido pornográfico. El afectado recurrió

---

[490] Para ver con más detalle este tema, remitirse a la obra de CUERVO, José, ***La Intimidación Informática del Trabajador***, Revista de Derecho Informático, No. 003, octubre de 1998, http://www.alfa-redi.org/rdi-articulo.shtml?x=158

[491] Para mayor información ver la obra de RUBIO DE MEDINA, María Dolores, ***El despido por utilización personal del correo electrónico***, Editorial Bosch, España, 2003.

ante el juzgado de Instrucción Segundo de Barcelona, y posteriormente. Ante le Tribunal Superior de Justicia de Cataluña, 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". [492]

El informe de la Fiscalía de Cataluña sentenciaba 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.[493]

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 Cataluña 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 Cataluña, la medida de control informático de la empresa era "justificada (ya que existían razonables

---

[492] Sentencia dictada por la Sala de Social del T.S.J. de Catalunya de fecha 14/11/2000, conocida también como "**La sentencia de los *emails***", pág. 11. http://www.abog.net/documentos/documentos_emails_1.asp

[493] La información de este caso de obtuvo de el diario español "Elmundo.es" la nota se titula "***La Fiscalía entiende que no es delito que los jefes controlen los emails de sus empleados***" http://www.elmundo.es/navegante/2001/11/26/esociedad/1006801495.html de fecha 26 de noviembre de 2001.

sospechas de la comisión por parte del empleado de grave irregularidades en su puesto de trabajo."[494]

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 encontramos, ya sea en nuestra casa, en nuestro trabajo, en nuestro automóvil o 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 consientes que la computadora, así como ejemplo el fax o el teléfono son bienes que le pertenecen a la empresa y que tienen asignada una función determinada para su uso, el cual es el funcionamiento de ésta. De ello 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[495], 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 es una entrevista concedida al diario argentino Clarín[496] 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"[497] Continua el Juez argumentando que "si no se le da el debido

[494] **Sentencia del T.S.J. de Cataluña de 23 de octubre de 2000** (AS. 2000/4.536), por la que se declara de oficio la nulidad de la Sentencia del Juzgado de lo Social núm. 1 de los de Barcelona en demanda de despido disciplinario contra la empresa "PRODUCTOS EATON LIVIA S.A." formulada por el actor con antigüedad superior a 30 años, que era Jefe de Métodos y con salario mensual de 680.488 ptas.

[495] Una detallada exposición de este tema está en la publicación de HERRERA BRAVO, Rodolfo y HERNANDEZ RUBIO, Montserrat, ***La Legitimidad del Control Tecnológico del Empleador sobre el Trabajador***, Revista de Derecho Informático, No. 035, junio de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=709

[496] Esta información se obtuvo de la Columna de Opinión del diario argentino Clarín de fecha de diciembre de 2001, en entrevista al Juez del estado de Minnesota, James M. ROSENBAUM, en un artículo titulado "Ante todo, privacidad".

[497] El precedente del tema que se trata en esta entrevista es el siguiente: "Hace unos meses, 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

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".

En nuestro país no existe una regulación específica ni precedente alguno en jurisprudencia sobre el uso del correo electrónico e Internet en las relaciones laborales, la única disposición que existe es el artículo 135 de la Ley Federal del Trabajo que en su fracción IX, señala que el trabajador tiene la obligación de utilizar las herramientas de trabajo únicamente para el objeto para el que le fueron destinadas, por lo que se puede concluir que actuar en contra de lo que señala este numeral puede significar una causa de rescisión de contrato de trabajo sin responsabilidad alguna para el empleador. Al decir de Yesín Ramírez Chelala: "por lo que toca a la Ley Federal del trabajo, si bien es cierto que por analogía se le podría dar el carecer de herramienta de trabajo al correo electrónico e Internet, sería idóneo para efectos procesales, que en la misma Ley se adoptara dicha disposición, a fin de proteger a los patrones del uso indebido de las TICS por parte de los trabajadores, con el objeto de disminuir riesgos y responsabilidades que su uso indebido pueda conllevar".[498] Se puede decir que si el trabajador ocupa parte de su tiempo laboral en el uso de correo electrónico o consulta de Internet para fines personales desatendiendo sus labores pone en riesgo el patrimonio de la empresa actuando en contra de la fracción IV del numeral 134 del mismo ordenamiento legal que establece que el trabajador deberá ejecutar el trabajo con la intensidad, cuidado y esmero apropiados y en la forma, tiempo y lugar convenidos.

Ahora bien, el respeto a la vida privada de los trabajadores también tiene que ser garantizado, ya que Internet se puede convertir en medio de control de los trabajadores, como dijera Rocío Ovilla Bueno[499] "es necesario hacer respetar las reglas relativas a la protección de la vida privada y el secreto de correspondencias. El empresario o patrón no tiene el derecho de interceptar el correo electrónico de sus trabajadores, ya que puede tener una responsabilidad penal por abrir este correo de sus trabajadores", se refiere a la violación de correspondencia señalada expresamente en el artículo 16 de la Constitución Política,[500] pero como ya lo estudiamos es difícil hacer una analogía entre el correo convencional y el correo electrónico. Nuestro máximo tribunal, la Suprema Corte de Justicia de la Nación nos da luz en el tema y en un criterio establece lo siguiente:

> **VIOLACIÓN DE CORRESPONDENCIA, CONCEPTO DE CORRESPONDENCIA EN EL DELITO DE.** Para la configuración del

---

empleados del departamento fue despedidos". 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.

[498] RAMIREZ CHELALA, Yesín y VERA PRENDES, Luis, ***Aspectos Laborales de la sociedad de la información*** en NAVARRO ISLA, Jorge, (coord) ***Tecnologías de la Información y de las comunicaciones aspectos legales***, Editorial Porrúa, México, 2005, pág. 345.

[499] ***La protección de los datos personales en México***, Editorial Porrúa, Colección Breviarios Jurídicos No. 28, pág. 50.

[500] Artículo 16 constitucional párrafo decimosegundo: "La correspondencia que bajo cubierta circule por las estafetas estará libre de todo registro y su violación será penada por la ley". A su vez el Código Penal Federal en su artículo 173 sanciona al que abra indebidamente una comunicación escrita que no este dirigida a él.

> delito de violación de correspondencia es irrelevante que haya sido un sobre que contenía un giro telegráfico el que abrió indebidamente el inculpado, al no estar dirigido a él, toda vez que debe considerarse como correspondencia una comunicación escrita, entendiéndose por tal, una carta o comunicación con el sobrescrito cerrado o con la plica cerrada y sellada, un pliego igualmente guardado en el sobrescrito o la plica, un despacho telegráfico o telefónico con igual protección y cualquier otra comunicación escrita análoga[501]

En este orden de ideas solamente podrían ser revisadas dichas comunicaciones con el consentimiento del expreso del trabajador, ya que si no es de esta forma carecen de valor probatorio y son constitutivas de delito.
Desde mi punto de vista, debe preciarse que si es la empresa la que provee de computadoras a los trabajadores, y si ésta además les entrega una dirección de correo electrónico que incluso lleve dentro de la dirección el nombre de dicha entidad (ejemplo:jimenezgl@unistudios.com), 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 facilitan. Dentro de la doctrina, 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.

Además de lo anterior comparto la postura de Rocío Ovilla Bueno, en el sentido de que el empresario realice una cláusula en el contrato de trabajo donde se precise claramente cuáles son las posibilidades para que el trabajador utilice la mensajería electrónica de la empresa, así como los derechos que tienen el empresario para leer este tipo de correo profesional.

VII.- Internet y los Órganos Gubernamentales:

Muchos entes policiales e investigativos utilizan Internet, conscientes 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

---

[501] Tesis aislada, ***Semanario Judicial de la Federación y su Gaceta***, t. VIII, junio de 1991, Octava Época, tribunales colegiados de circuito, p. 459.

ciberespionaje.[502] Y es que efectivamente, la red muchas veces ha sido utilizada como medio para la comisión de ilícitos como pornografía infantil, 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 sitios de Internet, se revelaba información para cometer estos actos, como por ejemplo los planos de un avión, indicaciones precisas del actuar de los terroristas, etcétera. Ello ha motivado a que órganos gubernamentales, para contrarrestar este tipo de actos, utilicen 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 pude tener acceso a todo tipo de comunicaciones enviadas a través de Internet, según pruebas recientes. Un oficial del FIB que participó en las pruebas señaló que aunque *Carnivore* tiene la habilidad de grabar una gran cantidad de mensajes de correo electrónico 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 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."[503] Sin embargo, aún cuando en teoría estos mecanismos de rastreo debieran ponerse instalarse solamente previa autorización por parte de 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".[504] Efectivamente, el control de la red es una tarea muy difícil de logra, 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

---

[502] La palabra *cyber* o *ciber* se define como un "Prefijo utilizado ampliamente en la comunidad Internet para denominar conceptos relacionados con las redes (ciberespacio, cibernauta, etc,) su origen es la palabra griega *kibernao*, que significa pilotar una nave". ***Glosario básico inglés – español para usuarios de Internet***, Asociación de Técnicos de Informática de España, de esta raíz es que se ha formado el término ciberespionaje. http://www.ati.es/novatica/glosario/glosario_internet.html#indice

[503] ***Desastre 11-S. Como afectará este ataque el futuro de Internet***, página de noticias Informáticas, Micro Tecnologías, el 12 de septiembre de 2001. Pero nuestros procedimientos son muy detallados, solamente hacemos lo que nos está permitido por la orden de la corte http://www.microteknologias.cl/rep_carnivore.html

[504] SÁNCHEZ ALMEIDA, Carlos, ***Intimidad: Un derecho en Crisis. La Erosión de la Privacidad***, Revista de Derecho Informático, No. 024, julio del 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=504

Internet),[505] los gobiernos no van a dar su brazo a torcer en este campo. Sánchez Almeida, refiriéndose a estos órganos argumentaba que "Mucho se 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 derecho 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".[506]

Es nuestro país para garantizar la presencia de la autoridad en la supercarretera de la información, la Policía Federal Preventiva desarrolló en México la primera Unidad de Policía Cibernética,[507] que además de las acciones preventivas en

---

[505] **ECHELON** es la mayor red de espionaje y análisis para interceptar comunicaciones electrónicas de la historia. Controlada por la comunidad UKUSA (Estados Unidos, Canadá, Gran Bretaña, Australia, Irlanda del Norte y Nueva Zelanda), ECHELON puede capturar comunicaciones por radio y satélite, llamadas de teléfono, faxes y *emails* en casi todo el mundo e incluye análisis automático y clasificación de las interceptaciones. Se estima que ECHELON intercepta más de tres mil millones de comunicaciones cada día. A pesar de haber sido presuntamente construida con el fin de controlar las comunicaciones militares y diplomáticas de la Unión Soviética y sus aliados, se sospecha que en la actualidad ECHELON es utilizado también para encontrar pistas sobre tramas terroristas, planes del narcotráfico e inteligencia política y diplomática. Sus críticos afirman que el sistema es utilizado también para el espionaje económico y la invasión de privacidad en gran escala. Los miembros de esta alianza de habla inglesa son parte de la alianza de inteligencia UKUSA, que lleva reuniendo inteligencia desde la Segunda Guerra Mundial. La existencia de ECHELON fue hecha pública en 1976 por *Winslow Peck*. Varias fuentes afirman que estos estados han ubicado estaciones de intercepción electrónica y satélites espaciales para capturar gran parte de las comunicaciones establecidas por radio, satélite, microondas, celulares y fibra óptica. Las señales capturadas son luego procesadas por una serie de supercomputadoras, conocidas como *diccionarios*, las cuales han sido programadas para buscar patrones específicos en cada comunicación, ya sean direcciones, palabras, frases o incluso voces específicas. El sistema está bajo la administración de la NSA (*National Security Agency*). Esta organización cuenta con 100.000 empleados tan sólo en Maryland (Estados Unidos) (otras fuentes hablan de 38.000 empleados a escala mundial), por lo que es probablemente la mayor organización de espionaje del mundo. A cada estado dentro de la alianza UKUSA le es asignado una responsabilidad sobre el control de distintas áreas del planeta. La tarea principal de Canadá solía ser el control del área meridional de la antigua Unión Soviética. Durante el período de la guerra fría se puso mayor énfasis en el control de comunicaciones por satélite y radio en centro y Sudamérica, principalmente como medida para localizar tráfico de drogas y secuaces en la región. Los Estados Unidos, con su gran cadena de satélites espías y puertos de escucha controlan gran parte de Latinoamérica, Asia, Rusia asiática y el norte de China. Gran Bretaña intercepta comunicaciones en Europa, Rusia y África. Australia examina las comunicaciones de Indochina, Indonesia y el sur de China, mientras que Nueva Zelanda barre el Pacífico occidental. Según algunas fuentes el sistema dispone de 120 estaciones fijas y satélites geoestacionarios. Estos podrían filtrar más del 90 % del tráfico de Internet. Las antenas de Echelon pueden captar ondas electromagnéticas y trasmitirlas a un lugar central para su procesamiento. Se recogen los mensajes aleatoriamente y se procesan mediante los diversos filtros buscando palabras clave. Este procedimiento se denomina "Control estratégico de las telecomunicaciones". ***Wikipedia. La enciclopedia libre,*** http://es.wikipedia.org/wiki/ECHELON

[506] SANCHEZ ALMEIDA, Carlos, Ibídem

[507] Entre sus principales funciones están: "Identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como a la elaboración, distribución y promoción de pornografía infantil, por cualquier medio. Localización y puesta a disposición ante autoridades ministeriales de personas dedicadas a cometer delitos informáticos. Realización de operaciones de patrullaje *anti hacker*, utilizando Internet como instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red. Análisis y desarrollo de investigaciones en el campo sobre las actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil". Información de la página de la Secretaria de Seguridad Pública: http://www.ssp.gob.mx/portalWebApp/appmanager/pcibernetica/desk?_nfpb=true&_pageLabel=pcibernetica_page_3&docName=¿Quiénes%20somos?&nodeId=/BEA%20Repository/99424//archivo&pathImg=/BEA%20Repository/Import/Policia%20Federal%20Preventiva/Policía%20Cibernética/Conoce%20a%20la%20Policía%20Cibernética/¿Quiénes%20somos?

materia de delitos cometidos en Internet y usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra menores, como existen en los países desarrollados.

Los crímenes cometidos en agravio de menores a través de una computadora y otros medios han tenido un incremento sin precedentes, tanto en México como en el mundo, derivado de la velocidad del desarrollo tecnológico y con las crecientes oportunidades de acceso a Internet. La red ha sido utilizada por organizaciones criminales de pedófilos que promueven y transmiten pornografía infantil; también, se sabe de las operaciones de bandas internacionales de prostitución, que utilizan sistemas informáticos como medio de promoción y sobre todo de reclutamiento. Otro tipo de crímenes que se han incrementado de manera considerable son el fraude cibernético, la piratería de software, la intrusión a sistemas de cómputo, el *hackeo*, la venta de armas y drogas por Internet y el ciberterrorismo que en los últimos años ha cobrado mayor importancia y es un tema aparte que requiere de un estudio minucioso, solo por dar un ejemplo debemos citar una amplia investigación que realizó el diario nacional "El Centro"[508] en su edición de lanzamiento, donde se señala que "un informe del Departamento de Justicia de EU, fechado el 5 de septiembre de 2006 confirma que el FBI opera una oficina especial de investigación y lucha antiterrorista desde los atentados de Nueva York, en 2001. El gobierno de México siempre lo ha negado." Pero esto no es lo más alarmante si no la posibilidad que tienen de violar la vida privada de las personas simplemente por creer que tienen alguna relación terrorista, así continúa la nota: "el gobierno mexicano ha permitido a Verint Technology Incorporation[509] realizar acciones de espionaje en el territorio nacional, mediante la intervención de líneas telefónicas, lectura de correos electrónicos, navegación en todas las páginas *web* e intervención en llamadas a celulares en todo el país –cuando el FBI y la Procurduría General de la República consideren que hay reisgo para la seguridad de Estados Unidos y Canáda".[510] Como podemos observar la creación de estas policías es benefica en algunos aspectos pero en otros menoscaba los derechos fundamentales de los ciudadanos en concreto el derecho a la vida privada

Sin embargo, el problema está en que la información que estos perciben muchas veces ha sobrepasado los límites puramente investigativos y se vuelven verdaderos sistema 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

---

[508] HERNANDEZ, Luis Guillermo, ***El vigilante que todo lo ve y lo oye,*** "El Centro"; México, lunes 5 de marzo de 2007, pág. 2 y 3.

[509] Verint Technology Inc, subsidiaria de Verint Systems Inc, es una empresa fundada en 1994 con capital privado en la que participan como accionistas funcionarios y ex funcionariso de Washington, de acuerdo con un reportaje de Robert O´Harrow Jr, del Centro de Reporteros de Investigación de Estados Unidos.

[510] HERNANDEZ, Luis Guillermo, ***También husmea el FBI,*** "El Centro", México, martes 6 de marzo de 2007, págs. 2 y 3.

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 caso 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 al a 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"[511]. 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 mismo, sino como fines en sí mismo, sino como bienes intermedios para lograr otros fines. Desde esta 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"[512]

La postura de Posner se sintetiza, básicamente enfocando al derecho a la vida privada sustentado en la eficiencia económica (donde la gente se vendría a sí misma tanto como a sus bienes), y según los siguientes principios: "I) 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,

---

[511] POSNER, Richard, ***The Right of Privacy***, en Georgia Law Review, 12(3), 1978, pág. 394.

[512] CORRAL TALCIANI, Hernán, en ***Configuración Jurídica del Derecho a la Privacidad II***, Revista Chilena de Derecho, Vol. 27 No.2, pág.72, Sección Estudios. 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 cuotas 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 fisgón."

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 intrusitos; 3)limitar, tanto como sea posible, las escuchas comunicacionales y otras formas de vigilancia intrusiva a la vigilancia de actividades ilegales".[513]

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".[514]

Considero prudente, a modo de reflexión, tomar las palabras de 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"[515]. 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 se ha desarrollado en la actualidad justamente una fundamentación postmoderna, inclinada por sobre todo a la defensa de la dignidad humana frente a la amenaza 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"[516]

---

[513] POSNER, Richard, ***The Right of Privacy***, en Georgia Law Review, 12(3), 1978, pág. 399.
[514] Ibídem, refiriéndose básicamente a la obra de BLOUSTEIN, Edward, ***Privacy as dear at any price: a response to profesor Posner' s Economic Theory***, en Georgia Law Review 12, 1978, pág. 440.
[515] CORRAL TALCIANI, Hernán, en ***Configuración Jurídica del Derecho a la Privacidad II***, Revista Chilena de Derecho, Vol. 27 No.2, pág. 72.
[516] Ibídem, pág.73.

CAPÍTULO SEXTO

EN BUSCA DE SOLUCIONES PARA PROTEGER EL DERECHO A LA VIDA PRIVADA FRENTE A LAS NUEVAS TECNOLOGÍAS

"La persona que pierde su intimidad, lo pierde todo."
Milan Kundera

CAPÍTULO SEXTO. 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 vida privada han sufrido constantes amenazas. De esto son conscientes 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".[517]

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.

I.- 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

---

[517] H. GATES, William, ***Ensayo para el Presidente de Estados Unidos George W. Bush. Moldeando la era Internet***, Diario El Mercurio, 8 de febrero de 2000, pág. 16. Su versión online en Diario de la Sociedad Civil, http://www.sociedadcivil.cl/nuevodiario/sitio/informaciones/documento.asp?Id=127

manifiesten el grado de intimidad que requieren se les apliquen al hacer uso de la red. Es así que en mayo de 1998, el *World Wide Consortion*, o W3C[518] 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 cundo se conecte a un sitio *web*. El agente de usuario puede residir en el propio ordenador del usuario o en el del proveedor de servicio. Es 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) 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."[519]

Sin embargo, muchas dudas han surgido en cuanto a su efectividad, y una de ellas es que , según el profesor de la Facultad de Derecho de la Universidad de Miami Jeremy Birchman,[520] "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. 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*.

---

[518] El *World Wide Web Consortium*, abreviado **W3C**, es un consorcio internacional que produce estándares para la World Wide Web. Está dirigida por Tim Berners-Lee, el creador original de URL (*Uniform Resource Locator*, Localizador Uniforme de Recursos), HTTP (*HyperText Transfer Protocol*, Protocolo de Transferencia de HiperTexto) y HTML (Lenguaje de Marcado de HiperTexto) que son las principales tecnologías sobre las que se basa la Web. Definición de ***Wikipedia. La enciclopedia libre.*** http://es.wikipedia.org/wiki/World_Wide_Web_Consortium

[519] VILLATE, Javier, P3P, ***un estándar para la privacidad, ¿ Es lo que necesitamos?***, Revista de Derecho Informático, No. 001, agosto de 1998, http://www.alfa-redi.org/rdi-articulo.shtml?x=138

[520] BIRCHMAN, A. Jeremy, ***Is P3P "the devil"?***, University of Miami School of Law, May, 1998, http://personal.law.miami.edu/~froomkin/sem97/birchman.html

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 *TRUSTe*

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 7.0, 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* 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[521] o decodificar información codificada con la clave pública correspondiente. Al enviar un mensaje a otra persona, en realidad se le diría 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; si el sitio tiene conexión segura (o *Secure Sockets Layer* o SSL), que se comprueba a su vez con el respectivo certificado.[522] Un ejemplo en el ámbito nacional dentro de la rendición de cuentas de los servidores públicos es el sistema "Declaranet" donde cada servidor público cuenta con su firma electrónica, una llave pública, una privada

---

[521] DEL PESO NAVARRO, Emilio, la define como: "una señal digital representada por una cadena de bits que se caracteriza por ser secreta, fácil de reproducir y de reconocer, difícil de falsificar y cambiante en función del mensaje y en función del tiempo" ***Resolución de conflictos en el intercambio electrónico de documentos***, en Ámbito Jurídico de la información, Cuadernos de Derecho Judicial, Escuela Judicial-Consejo General del Poder Judicial, Madrid, 1996, pág. 191. Mi definición estudiada en el volumen: ***Hacia una regulación del comercio electrónico en México***, es la siguiente: "la firma electrónica supone una serie de características añadidas al final de un documento. Es elaborada según procedimientos criptográficos, y lleva un resumen codificado del mensaje, y de la identidad del emisor y receptor, Tesis de Licenciatura, México, 2000, pág. 283.

[522] Esta información es la que ofrece el navegador de Microsoft, llamado Internet Explorer 7.0

y su respectivo certificado que es autentificado por la Secretaría de la Función Pública.[523]

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 terceros; y finalmente, aquellos que se reservan la facultad de revelar todo tipo de información a terceras partes.[524]

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,[525] y en la actualidad en el ciberespacio. Se dice que la palabra criptología proviene de las palabras griegas *krypto* y *logos* y significa "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.[526]

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

---

[523] Para mayor información remitirse al sitio: www.declaranet.gob.mx

[524] VILLLATE, Javier ***P3P, un estándar para la privacidad, ¿ Es lo que necesitamos?,*** Revista de Derecho Informático, No. 001, agosto de 1998, http://www.alfa-redi.org/rdi-articulo.shtml?x=138 .Para tener más información sobre este sistema TRUSTe, remitirse a http://www.truste.org.

[525]Como ejemplo podemos citar a la máquina **Enigma** era un mecanismo de cifrado rotativo utilizado tanto para cifrado como para descifrado, ampliamente utilizada de varios modos en Europa desde los tempranos años 1920 en adelante. Su fama se la debe a haber sido adoptada por muchas fuerzas militares de Alemania desde 1930 en adelante. Su facilidad de manejo y su supuesta inviolabilidad fueron las principales razones para su amplio uso. Su cifrado, fue roto, y la lectura de la información que ofrecía en los mensajes que no protegió es a veces reconocida como la causa para acabar al menos un año antes la Segunda Guerra Mundial de lo que hubiera podido ser de otro modo. La máquina equivalente británica, Typex, y varias americanas, p.e. la SIGABA (o M-135-C en el ejército), eran similares en principio a Enigma, pero mucho más seguras. La primera máquina moderna de cifrado rotatorio, de Edward Hebern, era considerablemente menos segura, hecho constatado por William F. Friedman cuando fue ofrecida al gobierno de Estados Unidos. Para más información ver SEBAG-MONTEFIORE, Hugh, ***Enigma: The battle for the code,*** Published by Jhon Wiley & Sons, Hoboken, New Jersey, 2000.

[526] Para más información ver JIMENEZ GUZMAN, Luis, ***Hacia una regulación del comercio electrónico en México,*** Tesis de Licenciatura, México, 2000, Capítulo Tercero.

han propuesto programa como el PGP,[527] 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 computadoras descargando el programa a través de Internet.

Sin embargo, esta solución también ha 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 precio poco accesible lo cual degenerará en unos pocos afortunados que puedan pagar por su privacidad. Sin lo ofreciesen gratuitamente podrían pedir igualmente nuestros nombres para la licencia de uso (lo cual ocurre en cualquier utilitario al cual hagamos un *download*)."[528]

En México el Código de Comercio (Título Segundo, De Comercio Electrónico, reforma publicada en el Diario Oficial de la Federación el 29 de mayo de 2000) reconoce el uso de la firma electrónica,[529] la cual tiene gran aplicación en la sociedad, pero más bien enfocada a trámites frente al gobierno federal como las declaraciones de impuestos o en el derecho mercantil.[530] 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

---

[527] *Pretty Good Privacy* o PGP (*privacidad bastante buena*) es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales. PGP originalmente fue diseñado y desarrollado por Phil Zimmermann en 1991. El nombre está inspirado en el del colmado *Ralph's Pretty Good Grocery* de Lake Wobegon, una ciudad ficticia inventada por el locutor de radio Garrison Keillor. Utilizado correctamente, PGP puede proporcionar un gran nivel de seguridad. Es más, observadores informados creen que ni siquiera las agencias del gobierno estadounidense como la NASA son capaces de descifrar directamente mensajes generados adecuadamente con PGP. PGP es más fácil de utilizar que muchos otros criptosistemas, pero como ocurre siempre en el campo de la criptografía, su implementación y su utilización influyen muchísimo en la seguridad lograda. Existe la posibilidad de que haya errores en la implementación, y si se utiliza descuidadamente es posible desproteger fácilmente un archivo de texto protegido. Cualquier criptosistema puede ser inseguro, independientemente de lo bueno que sea su diseño. A diferencia de protocolos de seguridad como SSL, que sólo protege los datos *en tránsito* (es decir, mientras se transmiten a través de la red), PGP también puede utilizarse para proteger datos almacenados en discos, copias de seguridad, etcétera. ***Wikipedia. La enciclopedia libre***, http://es.wikipedia.org/wiki/Pretty_Good_Privacy Ver también el sitio oficial de PGP: http://www.pgpi.org/

[528] MENDOZA LUNA, Amílcar, ***Los Cookies ¿amenaza a la privacidad de información en la Internet?,*** Revista de Derecho Informático, No. 031, enero de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=612 .Aprovecho para explicar el significado de las siguientes palabras: Se define a *software* (programas, componente lógicos, *software*) como "Programas o elementos lógicos que hacen funcionar un ordenador o una red, o que se ejecutan en ellos, en 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.atl.es/novatica/glosario/glosario_internet.html

[529] Para más información ver: REYES KRAFFT, Alfredo, ***La firma electrónica y las entidades de certificación***, Editorial Porrúa, México, 2003 o ANDRÉS CAMPOLI, Gabriel, ***La firma electrónica en el régimen comercial mexicano***, Editorial Porrúa, México, 2004.

[530] Al respecto Reyes Krafft, nos dice que los objetivos de la reforma del 2000 son, "el reconocimiento de la validez jurídica del Contrato Electrónico; la posibilidad de exigibilidad judicial de los contratos realizados a través de medios electrónicos; medios probatorios del Contrato Electrónico y valoración de la prueba en juicio; así como una protección razonable a los consumidores" REYES KRAFFT, Alfredo, ***La firma electrónica y las entidades de certificación***, Editorial Porrúa, México, 2003, pág. 55.

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 determinada 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 le 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."[531]

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 reclamación 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."[532]

II.- Soluciones jurídicas

1.- Los Códigos de Conducta

Estos códigos, llamados también "Códigos Deontológicos", han sido aplicados en distintos ordenamiento 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 la particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva".[533]

---

[531] JIJENA LEIVA, Renato, ***Responsabilidad de los ISP por la difusión de contenidos on line***, Revista Electrónica de Derecho Informático, No. 15, octubre de 1999, http://premium.vlex.com/doctrina/REDI-Revista-Electronica-Derecho-Informatico/Informe-legal-Improcedencia-censurar-legalmente-contenidos-Internet-Analisis-Boletin-N%B02395-19/2100-107405,01.html

[532] Ibídem

[533] Extracto del Artículo 27 de la Directiva 95/46/CE de la Unión Europea.

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."[534] Como lo señala la mencionada autora, éstos códigos no son ajenos a lo que las 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 Herrán Ortiz, "Ha merecido importancia 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."[535]

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 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 sus confianzas, 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

---

[534] HERRÁN ORTIZ, Ana Isabel, ***El derecho a la protección de datos personales en la sociedad de la información***, Universidad de Deusto, Bilbao, España, 2003, pág. 21.
[535] Ibídem.

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."[536]

Dentro la doctrina, 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 autorregulación. 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 sea aceptada mundialmente por los usuarios de la red. Así ha ocurrido con la 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 actúan 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 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 sí 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 "autorregulación 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 específicas detrás que permita al usuario consultar la base de datos y ver qué tiene la empresa sobre él, saber qué sucede 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

---

[536] H. GATES, William, ***Ensayo para el Presidente de Estados Unidos George W. Bush. Moldeando la era Internet***, Diario El Mercurio, 8 de febrero de 2000, pág. 12. Su versión online en Diario de la Sociedad Civil, http://www.sociedadcivil.cl/nuevodiario/sitio/informaciones/documento.asp?Id=127

discriminación por status socio-económico. Como hemos dicho ya varias veces, vender datos personales es uno de posnegocios 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 basen de datos de medio mundo."[537]

Soy 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 de datos de carácter personal son muy cotizados en el ciberespacio. Insisto en las palabras de Stephen Lau,[538] la tentación es demasiado grande... sobre todo en una sociedad como la nuestra donde el proverbio de que información es poder cobrar más fuerza cada día. 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".[539] 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 otros Estado que les acuerdo una protección sustancialmente equivalente a la que reciben en el país exportador); la recomendaciones de la OCDE que establecería en su artículo 17 el "principio de la equivalencia", más tarde recogidas por la ONU, y que en realidad se han traducido en "busca 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".[540]

---

[537] CASACUBERTA, David, ***La privacidad en los nuevos medios electrónicos. Aspectos éticos y sociales***, Revista de Derecho Informático, No.011, Junio de 1999. http://www.alfa-redi.org/rdi-articulo.shtml?x=276

[538] Para más información al respecto ver: LAU, Stepehn, ***Comercio electrónico, derecho del consumidor y protección de datos***, Memorias de la XX Conferencia Internacional de Autoridades de Protección de Datos, Santiago de Compostela, España, 1998

[539] Según el artículo 25 de la Directiva de la Unión Europea, transferir los datos hacia países con unas salvaguardas menos rigorosas 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.

[540] DIAZ ARIAS, Rafael, ***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, Revista de Derecho Informático, No. 023, Junio de 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=488 Para ver con más detalle los

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 transformara datos de carácter personal a empresa u organizaciones que, a través de un auto declaración o auto certificación 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 par las multinacionales, que al estar establecidas en Europa, se supone que no podían transmitir 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.

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 aterritorial, 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", encargada de combatir los ilícitos que se susciten en la red, misma de la que ya se abordo en páginas anteriores.

Es solución ha sido ya considerada en algunos países, y de hecho en la actualidad existe un proyecto llamado GIG, 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 dicte sus propias normas respetando siempre las directrices que este Tratado Internacional llegara a imponer. De hecho, aún cuando este principio ya ha

---

textos de los organismos citados, remitirse a la obra de URIOSTE, Mercedes, ***Protección de Datos Personales***, Investigaciones 1, Subsecretaría de Investigación en derecho comparado de la CSJN, Buenos Aries, Argentina, 1998, pág. 5.

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,[541]"toda negociaciones 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 negociación privadas sean cero; y 2) que la asignación de los derechos, obligaciones y responsabilidades de las partes sea bien delimitada[542]. 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 o responsabilidades legales entre las partes, con la finalidad de facilitar el proceso negociador. Así, la

---

[541] R. GIESZE, Craig, ***El análisis económico de la información privilegiada en el mercado de capitales y valores:¿Justicia ineficiente?***, Revista Chilena de Derecho, Vol.26 No 4, Chile, 1999, pág.823.

[542] 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 siguiente 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.

aplicación normativa del Teorema de Coase puede fomentar la adopción de transacciones extrajudiciales eficiente entre los particulares[543]".

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 lícitos. 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 pueden 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 definitivamente altos; 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 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 consecuencias de ello, las medidas a tomar por parte de un Estado, por ejemplo el mexicano, 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 o pasivos en el uso de Internet, determinando así el rol que cada uno de ellos tiene.

---

[543] 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 en las negociaciones; 4) mal ambiente negociador; 5) poco conocimiento entre los negociadores ; 6)comportamiento razonable; 7) intercambios a lo largo de tiempo; 8) falta de contingencias; 9)bajo costo de monitores; y 10) castigos de alto costo.

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 de México en espacial, creo que hay muchas cosas que hacer en el camino. Una de ellas es modificar la Constitución como ya quedo propuesto en el Senado, luego promulgar una ley de protección de datos de tal manera que se adapte a las exigencias internacionales que otros ordenamientos como los europeos han establecido en este sentido. México no puede considerarse en este momento como un "puerto seguro" para quienes pretendan llevar a cabo un transferencia de datos desde un país que sí cumpla con estas políticas.

Además, en nuestro país 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.

6.- La creación de una autoridad de control en el ámbito nacional.

La necesidad de disponer de una autoridad de control ha sido reconocida por Naciones Unidas, en el principio octavo de las Directrices *para la regulación de los archivos de datos personales informatizados*, adoptadas mediante resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990, que establece que el derecho de cada país deberá designar a la autoridad que, de acuerdo con su sistema jurídico interno, vaya a ser responsable de supervisar la observancia de los principios de protección de datos. Esta autoridad deberá ofrecer garantías de imparcialidad, independencia frente a las personas o agencias responsables de procesar y establecer los datos, y competencia técnica.

Recientemente ha sido ratificada en la XXVII Conferencia Internacional de Autoridades de Protección de Datos celebrada en Montreux, Suiza, los días 13 a 15 de septiembre de 2005, en la que se aprobó una Declaración Final sobre *"The protection of personal data and privacy in a globalised world: a universal right respecting diversities"*.[544] En la Declaración se hace una referencia expresa al principio de supervisión independiente como uno de los principios del derecho a la protección de datos, y concluye apelando a todos los gobiernos a adoptar mecanismos legales de privacidad y protección de datos con el objeto de dar cumplimiento entre otros, al citado principio de supervisión independiente.

A) El Modelo europeo

[544] ***Montreaux Declaration***, Wednesday 21 December 2005, 27th International Conference of Data Protection and Privacy Commissioners, http://www.libertysecurity.org/IMG/pdf/montreux_declaration_eng.pdf

Para definir los elementos fundamentales de una autoridad de control de datos personales se deben tener en consideración las previsiones del Convenio 108 del Consejo de Europa de 1981, *para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, y su Protocolo adicional que estableció claramente la necesidad de que existan en cada país autoridades independientes que supervisen la aplicación de las normas de protección de datos y sus características esenciales. Este mismo esquema sin alteración sustancial se recogió en la Directiva europea de protección de datos de 1995 (Directiva 95/46/CE).

La Carta de los derechos fundamentales de la Unión Europea, adoptada en Niza el 7 de diciembre de 2000, ratifica que el respeto de las normas de protección de datos quedará sujeto al control de una autoridad independiente.

La Directiva 95/46/CE establece la necesidad de que cada Estado Miembro cree una o más autoridades de protección de datos encargadas de vigilar la aplicación en su territorio de las disposiciones de protección de datos. Estas Autoridades deben desempeñar sus funciones con total independencia; deben tener poderes de investigación (recabar toda la información necesaria para el cumplimiento de su misión de control); poderes efectivos de intervención (formular dictámenes antes de realizar los tratamientos); y capacidad procesal en caso de infracciones a las disposiciones nacionales. Las Autoridades deben atender todas las solicitudes de las personas afectadas en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Sobre la publicidad y transparencia de su actividad, la Directiva señala que deben presentar periódicamente -en la práctica es anualmente- un informe sobre sus actividades. Además, se promueve y habilita la cooperación entre diferentes Autoridades, en la medida necesaria para el cumplimiento de sus funciones, y en particular, mediante el intercambio de información que estimen útil. Como garantía de confidencialidad, la Directiva establece que los miembros y agentes de las autoridades de control estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso.

A este modelo que hemos descrito responde básicamente la Agencia Española de Protección de Datos[545] cuyo marco normativo se encuentra en la Ley Orgánica de Protección de Datos de 1999 (LOPD).
Sus notas características son:

- Es una Autoridad independiente.
- Presidida por un Director que es elegido entre los miembros de un Consejo Consultivo por 4 años.
- Sus decisiones sólo pueden ser revocadas por la Audiencia Nacional.
- En relación con la transparencia en su actividad, tiene la obligación de presentar una Memoria Anual en el Parlamento, que se difunde *on-line*. También se da difusión a los informes legales de la Agencia, y las resoluciones sancionadoras, que pueden servir de guía para los ciudadanos

[545] Más información en el sitio de la Agencia Española de Protección de Datos: www.agpd.es

y fijan una doctrina de actuación consolidada. Todo ello con respeto a las garantías de privacidad de los afectados (se disocian los datos personales citados en las resoluciones).
- La AEPD cuenta con poderes de supervisión (investigaciones, inspecciones, sanciones, etc.).
- Garantiza la publicidad de los tratamientos de datos personales existentes, a través del Registro General de Protección de Datos.
- Facilita a los ciudadanos la tutela de sus derechos y resuelve las denuncias de vulneración de la LOPD.
- Se financia a cargo de un presupuesto anual a cargo de los Presupuestos Generales del Estado y mediante otros sistemas de autofinanciación.

Junto al marco normativo de la LOPD, desde el año 2003, la Agencia Española tiene nuevas responsabilidades que afectan a la privacidad en las telecomunicaciones y que le han sido atribuidas por la Ley 32/2003 General de Telecomunicaciones, y la Ley 34/2002 de Servicios de la Sociedad de la Información. Fundamentalmente estas competencias se refieren a la vigilancia frente a las comunicaciones electrónicas no solicitadas ("*spam*").

También se corresponde con el modelo europeo la Comisión Nacional de Protección de Datos de Portugal,[546] creada mediante la Ley 67/98 de Protección de Datos Personales.

Asimismo, aunque no se encuentra integrada en la Unión Europea, en aplicación de la Ley 15/2003, de protección de datos personales, ha sido creada la Agencia Andorrana de Protección de Datos.[547]

B) La situación en Latinoamérica

La mayoría de las Constituciones de los Estados Latinoamericanos garantizan el derecho a la intimidad y privacidad y, explícita o implícitamente, la protección de los datos personales; pero carecen de leyes especiales en la materia, salvo en algunos casos excepcionales. Esto ha propiciado que una gran parte de los propios Estados Latinoamericanos no dispongan de autoridades que tengan como cometido sustantivo y especial el control de datos personales.

Caso especial es el de Argentina que cuenta con la Dirección Nacional de Protección de Datos Personales, como un órgano descentralizado del Ministerio de Justicia y Derechos Humanos de la Nación, con autonomía funcional y dirigido por un Director elegido por el Ejecutivo con concurso de oposición para un período de cuatro años (artículo 29 de la Ley 25.326).

La Dirección Nacional de Protección de Datos Personales,[548] creada por decreto reglamentario 1558/2001, goza de atribuciones de investigación e intervención, así como funciones de asistencia y asesoramiento. Puede adoptar normas y

[546] Más información en el sitio de la Comisión Nacional de Protección de Datos de Portugal: http://www.cnpd.pt/
[547] Más información en el sitio de la Agencia Andorrana de Protección de Datos: https://www.apda.ad/index.htm
[548] Consultar el sitio: http://www.jus.gov.ar/dnpdpnew/ para mayor referencia al respecto.

reglamentaciones para el desarrollo de la Ley, e implementa el Registro de bases de datos públicas y privadas. Además el órgano de control puede constituirse como denunciante en acciones penales, controlar el cumplimiento de los requisitos y garantías para inscribir bancos de datos en el Registro e imponer sanciones.

C) El modelo de los Estados Unidos de América

Como ya hemos estudiado, en los Estados Unidos, existe la ausencia de un régimen normativo que sea amplio y abarque la generalidad de las situaciones en protección de datos personales, hemos estudiado que la autorregulación ocupa el papel más importante, sobre todo dandole mayor peso e importancia a las empresas para que creen sus códigos de conducta (por ejemplo *TRUSTe*). Para apoyarnos en este tópico es interesante citar los dicho por De Miguel Asensio: "En EEUU el modelo imperante en la actualidad se caracteriza por la creciente aparición de normas, en gran medida como consecuencia de la autorregulación y de criterios desarrollados por la propia industria, tendentes a garantizar un mayor respeto a al intimidad de los usuarios".[549] En este orden de ideas la publicación de "políticas de privacidad" en los sitios *web* informa a los usuarios sobre la forma en que sus datos serán utilizados y si están de acuerdo en dichas medidas. Situación que no es del todo optima ya que no existe un verdadero control sobre las empresas en este tema.

D) Ponderación para la elección de un modelo

Más allá de las señaladas ventajas que proporciona la existencia de una autoridad de control para garantizar que los datos de carácter personal de los individuos serán utilizados en forma leal y lícita, y que estos contarán con herramientas y recursos efectivos para hacer valer sus derechos, su creación genera también una mayor confianza en los agentes involucrados en las transacciones comerciales, lo cual facilita el flujo internacional de datos imprescindible hoy en día en las relaciones económicas globales.

En este sentido conviene recordar que uno de los requisitos para que un tercer país pueda ser considerado por la Unión Europea con un nivel de protección adecuado es la existencia misma de una autoridad de supervisión dotada de auténticos poderes de control y que actúe con independencia en el ejercicio de sus funciones.

E) Alternativas

Alternativa 1: Utilizar la estructura administrativa, constitucional y judicial ya existente.

- Las funciones esenciales de la Autoridad, descritas en el modelo europeo pueden ser asumidas por órganos administrativos ya existentes –no específicos de protección de datos- siempre y cuando se arbitre un

[549] DE MIGUEL ASENSIO, Pedro Alberto, ***Derecho del comercio electrónico***, Editorial Porrúa, México, 2005, pág. 168.

mecanismo que garantice su independencia. En nuestro caso implica darle facultades al IFAI o tal vez a alguna dependencia gubernamental como lo es la Procuraduría Federal de Protección al Consumidor.

- Asunción de funciones por órganos constitucionales que tienen encomendada la protección de los derechos fundamentales (defensorías del pueblo, ministerios públicos, etc) de sus ciudadanos. En nuestro caso a la Comisión Nacional de Derechos Humanos.
- Articulación de mecanismos judiciales rápidos y gratuitos de defensa de la protección de datos y *habeas data*. Dotar de facultades a juzgados de primera instancia en materia civil para conocer de *habeas data* o en su caso hacer un recurso extensivo dentro de las atribuciones del IFAI.

Alternativa 2: Crear órganos y mecanismos complementarios de protección en el ámbito público.

- Al implementar las políticas de gobierno electrónico y modernización del estado debería tenerse muy en cuenta las implicaciones en el ámbito de la protección de datos y se podría sopesar la posibilidad de crear supervisores o encargados de la protección de datos en este ámbito. Sería el caso de la Instituto de Protección de Datos que contiene la Iniciativa García Torres, que es como hemos dicho una copia de la estructura española
- Reestructuración de órganos administrativos ya existentes creando nuevas unidades que no supongan incremento del gasto público pero sí racionalización de bienes materiales y personales para garantizar un derecho fundamental cuyo compromiso ha sido asumido al más alto nivel en la Declaración de Santa Cruz de la Sierra y debe traducirse en realizaciones concretas.

Alternativa 3: Promover una mayor colaboración del sector privado.

- Favorecer el funcionamiento de expertos u "oficiales de protección de datos" como medio eficaz de alcanzar mayores niveles de cumplimiento.
- Incentivar la autorregulación por los propios agentes interesados, por ejemplo, a través de códigos de conducta. Seguir el modelo de los Estados Unidos de América.

Es deber del Estado velar porque sus miembros gocen y ejerzan derechos como el de tener una vida privada, indispensables 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, incluyendo el nuestro. 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 ésta 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 nuestra vida cotidiana, y de las desventajas que éstas también acarrean consigo. La tarea es grande y el camino es largo.

CONCLUSIONES

CONCLUSIONES

- El concepto de vida privada ha evolucionado de manera radical en relación a sus primeras manifestaciones, hasta llegar a los avances tecnológicos de nuestros días.
- Los 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", con la llegada del mundo cristiano el reconocimiento de la intimidad se descubre como sustancia del alma.
- Entre el periodo que va desde el Renacimiento hasta el Siglo de las Luces, tomaría forma paralelamente la aparición de la vida pública de la 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, lograron en el hombre de la época que el recogimiento y la reflexión formen parte de su vida.
- *The Right to Privacy*, de Samuel D. Brandies, es un modelo prototípico del *Case Law*, de principios creados por vía inductiva a partir de precedentes, del cual derivan grandes pautas para la posterior evolución del derecho a la vida privada.
- 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 se tornó bastante más sofisticada de lo que se conocía hasta entonces.
- Dentro de la doctrina se señala que "en esta fase (la de los derechos de tercera generación), y dado el desarrollo tecnológico, toma mayor auge el reconocimiento del derecho a la intimidad surgiendo así nuevos perfiles del mismo y que por ende, exige un reconocimiento en sede constitucional, 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.
- 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 y como sinónimos.
- La intimidad: es donde el individuo ejerce plenamente su autonomía personal; es el reducto último de la personalidad, es allí donde soy lo que soy. (Ernesto Garzón Valdez)
- La privacidad es el: término al que podamos 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 tiene 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 ámbito de privacidad. (Davara Rodríguez)

- La vida privada es la "esfera personal exclusiva, jurídicamente reconocida y garantizada como derecho a todo ser humano, a fin de permitirle conducir una parte de su propia existencia de manera autónoma, independiente y libre de injerencias externas indebidas, en relación con algunas de sus convicciones, decisiones o actividades íntimas, o con sus relaciones o comunicaciones particulares, atributos personales, vida familiar, reserva domiciliaria, etc. (Diccionario Jurídico Mexicano).
- La doctrina 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". (Oscar Puccinelli)
- La autodeterminación informativa es: "aquel derecho que tiene por objeto garantizar la facultad de la personas para conocer y acceder a las informaciones que les concierne, 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".(Tribunal Constitucional Federal de Alemania).
- El *information control* se 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". (Pablo Lucas Murillo).
- El *habeas data* es un "recurso procesal diseñado para controlar la información personal contenida en bancos de datos, cuyo derecho implica la corrección, la cancelación y la posibilidad de restringir y limitar la circulación de los mismos." (Marcia Muñoz de Alba Medrano).
- En el caso del ordenamiento jurídico mexicano, los Tratados Internacionales tienen rango constitucional, y no obste decir que el derecho a la vida privada se encuentra contenido en instrumentos internacionales que México ha firmado en materia de derechos humanos.
- Dentro de los tratados signados entre México y la Organización de las Naciones Unidas existen varios instrumentos que protegen la vida privada de las personas, entre otros: la Declaración Universal de los Derechos Humanos.
- El reconocimiento a la protección a la vida privada en el ámbito de la Organización de Estados Americanos existen varios ordenamientos que vinculan a México para proteger este derecho fundamental, por ejemplo la Convención Americana de Derechos Humanos.

- La Organización para la Cooperación y el Desarrollo Económico adoptó la Declaración sobre flujos de datos transfronterizos, dicha declaración abordaba las cuestiones políticas que surgían del flujo de datos personales más allá de las fronteras nacionales como flujos de datos e información sobre actividades comerciales, flujos intraempresariales, servicios de información informatizada, e intercambios científicos y tecnológicos y posteriormente creó una comisión sobre informatización automatizada y privacidad.
- La Unión Europea tiene varios ordenamientos que protegen la privacidad de las personas como lo es la Convención Europea de Derechos Humanos y en específico a la protección de datos personales la Directiva 95/46.
- En Europa existen varios países que protegen la vida privada en específico en Internet, entre ellos: Italia, Alemania, Francia, Reino Unido, España entre otros.
- En América del Norte nuestros dos socios comerciales vía el TLCAN, protegen la vida privada de las personas en Internet, manejando modelos autorreguladores y con influencias del *common law.*
- En América latina encontramos países que regulan la protección a al vida privada en varios niveles, constitucional y legislación federal además de algunos países que reconocen el habeas data como una forma de defender este derecho fundamental. Entre ellos: Brasil, Ecuador y Argentina.
- El derecho a la vida privada 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 garantías. El ordenamiento jurídico mexicano no ha sido la excepción, y es así que el derecho a la vida privada de las personas ha encontrado un reconocimiento que cabe decir, no ha logrado ser expreso tanto a nivel constitucional como al nivel de otras normas de distinto rango.
- Un derecho fundamental son "todos aquellos derechos subjetivos que corresponden universalmente a todos los seres humanos en cuanto dotados de status de personas, de ciudadanos o de personas con capacidad de obrar". (Luigi Ferrajoli)
- La constitucionalización de un derecho supone, poner una determinada expectativa a un bien jurídico fuera del alcance del mercado y de la política ordinaria. Supone, por tanto, dejar a salvo de las fuerzas del dinero y de los intereses políticos determinado tipo de bienes, en nuestro caso los datos personales.
- Es importante destacar lo que ha sucedido en la doctrina internacional para la configuración de la protección de datos como un derecho fundamental, podemos decir que existe un desarrollo en la doctrina y en las normas acerca de este derecho. Al menos la Unión Europea lo considera un derecho fundamental.
- El sistema jurídico mexicano tiene un déficit normativo en lo que se refiere a la protección de la vida íntima de los mexicanos. En la

Constitución no se reconoce el derecho a la intimidad como fundamental, y se regula parcialmente como derivación de la tutela de otros derechos fundamentales, como la inviolabilidad de las comunicaciones privadas y la limitación a la libertad de imprenta.

- Podemos decir que el reconocimiento de la vida privada en la Constitución haría procedente el juicio de amparo en contra de actos de autoridad que violen el derecho a la vida privada de las personas y con ello conseguir la interrupción de las violaciones mediante la suspensión del acto reclamado. La experiencia de otros países como España, Alemania, Argentina o los Estados Unidos demuestran el funcionamiento que tiene este reconocimiento, limitando así los excesos de los factores de poder, como lo son los medios de comunicación o las empresas.
- La información judicial presenta la conflictiva relacionada a la protección de datos personales, abierta en dos dimensiones muy claras, por un lado la administración de recursos y la generación de políticas institucionales y la otra relativa al tratamiento de los datos que, como "Administradora de información pública y privada", adquiere y genera en el ejercicio de su función jurisdiccional.
- El caso de México y tomando como ejemplo nuestra Suprema Corte de Justicia y los Tribunales Agrarios, que han vivido un proceso de autonomización e independencia que sigue su marcha.
- El Tribunal Superior Agrario ha hecho esfuerzos para transparentar más la información que genera sin violentar la vida privada de los justiciables.
- El proceso de la transparencia y la apertura del Poder Judicial no pueden ser absolutos, ya que el derecho a la privacidad debe ser tutelado, hay ciertas informaciones que deben permanecer bajo sigilo.
- Es notorio que un pendiente nacional tanto a nivel local como federal es poner disponible en los sitios de Internet de los poderes judiciales información suficiente para enriquecer la interacción entre el trabajo del juzgador y los distintos sectores de la sociedad.
- A la fecha existen varias iniciativas para reconocer la protección de datos personales como un derecho fundamental, destacando la presentada el 5 de abril de 2006 por el Senador García Torres, misma que fue aprobada por el Senado, ahora tiene que seguir el tramite en la Cámara de Diputados. Pero a la vez existen varias más que no han tenido trámite alguno.
- La protección constitucional a la privacidad se traduce en realidad a una protección a la persona misma y a su intimidad. La Constitución garantiza, con ello, incluso el carácter secreto de las comunicaciones privadas, la inviolabilidad del domicilio entre otros derechos que tienden a la protección a al vida privada pero no existe una expresión directa a los datos personales.
- La protección a la vida privada se encuentra aislada en la legislación federal, así podemos mencionar múltiples ordenamientos que la regulan pero ninguno con expresión directa a datos personales, si algunas a medios electrónicos como lo es Internet o las telecomunicaciones.
- Existen varias iniciativas de Ley Federal de Protección de Datos Personales, ninguna de ellas ha sido aprobada por el poder legislativo.

- El Estado de Colima ha aprobado su Ley de Protección de Datos Personales, dando el ejemplo a seguir en materia federal.
- El éxito de Internet es la libertad que ofrece. No existe ninguna compañía u organización que posea o controle Internet. No hay censura, no hay jefes, ni directores ni accionistas. No hay costos por largas distancias, ni costo por tiempo de acceso; el costo solamente depende de la integración de servicios que se desea obtener y su nivel de conexión, Internet se ha convertido en un auténtico fenómeno social en México. Ha tardado bastante tiempo pero finalmente ha entrado desde las universidades, a las empresas, a los centros educativos y a los hogares.
- Una red de computadoras es la interconexión de varios computadoras, donde cada uno de ellos puede interactuar con los demás, a través de un medio de transmisión, con el fin de intercambiar información y compartir recursos como impresoras o programas, para que un usuario pueda utilizar Internet es necesario que tenga una forma de acceso. A esta forma en conjunto se le conoce como cuenta en Internet y esta puede ser contratada con un Proveedor de Servicios de Internet, que es una organización comercial cuya principal finalidad consiste en proveer el servicio de conexión a Internet entre sus clientes sean personas físicas o morales.
- Acceder a la red Internet y "*navegar*" por ella no supone otra cosa más que enviar y recibir información a los distintos ordenadores que hay conectados a la misma los cuales se llaman servidores.
- El correo electrónico nos permite enviar mensajes (y/o ficheros) como si de correo postal se tratara, pero con la diferencia de que se recibirán inmediatamente después de mandarlos y prácticamente nunca se pierde; *File Transfer Protocol* es el protocolo de Internet que permite conectarnos a ordenadores remotos y acceder a los ficheros que guardan para trasladarlos a nuestro ordenador o, a la inversa; el *World WideWeb* es un sistema basado en hipertexto que facilita la navegación por Internet. Pero, no sólo es hipertexto, es también hipermedia ya que permite acceder a información en formato multimedia digamos sonido, vídeo o la combinación de ambos; el *Internet Relay Chat* permite que diferentes usuarios mantengan conversaciones por escrito o vía voz en grupos temáticos o canales que pueden ser privados o públicos.
- Conocer el desarrollo histórico de Internet es fundamental, para así comprender como esta invención ha revolucionado a nuestro entorno actual y para posteriormente dilucidar como afecta a la vida jurídica dicho fenómeno, en particular los negocios en línea o comercio electrónico. Esta historia podemos decir que comenzó en los principios de los años sesenta, con el desarrollo de los programas de defensa norteamericanos y con ellos la aparición de ARPAnet.
- En la década de los noventa Internet se comercializa y expande al mundo deja las universidades y el ámbito público para convertirse del dominio privado. Acompañado de las actividades de comercio en línea, para los analistas de IDC, 1999 se destacará por el crecimiento acelerado y sostenido de Internet el cual llegará a los 147 millones de usuarios,

alcanzando los niveles de población de países como Rusia y Japón. También se destaca el hecho de que la mayoría de los usuarios de Internet vivirán fuera de los Estados Unidos, IDC predice que, por primera vez, la mayoría (51%) de los usuarios de Internet vivirán en otros países.

- La historia del Internet en México empieza en el año de 1989 con la conexión del Instituto Tecnológico y de Estudios Superiores de Monterrey, en el Campus Monterrey (ITESM), hacia la Universidad de Texas en San Antonio (UTSA), específicamente a la escuela de Medicina; nuestra máxima casa de estudios la UNAM fue la primera institución en todo el país en poseer un equipo de computo para investigación académica, el segundo logro para la historia de la informática en México fue el conformar el segundo nodo Internet en México siendo la Universidad Nacional Autónoma de México, donde se realizara esta conexión, en específico en el Instituto de Astronomía en la Ciudad de México.
- La aplicación de las nuevas tecnologías está generando nuevas formas de comportamiento y hábitos en todos los individuos. Es notorio que el ámbito jurídico global se ha fortalecido y México junto con América Latina están hoy inmersos en estos cambios. Es previsible que el mundo virtual traiga consigo cambios importantes en las instituciones jurídicas que existen en el país, así como el desarrollo de nuevas instituciones jurídicas que son el reto de los juristas del próximo milenio.
- En México, la palabra Internet es ignorada por nuestra legislación vigente. No existe un solo ordenamiento que mencione la palabra, ni existe ningún criterio jurisprudencial en función a su uso, ya que como señalamos, su utilización se había relacionado a un código ético y autorregulable. Sin embargo, es previsible en un futuro no muy lejano que el desarrollo del Internet traiga consigo cambios en las instituciones jurídicas nacionales, adaptándolas a la tendencia mundial de globalización de las telecomunicaciones que implica un irreversible proceso.
- Es un hecho que en 2006 los usuarios de Internet comenzaron a fortalecerse, la mayoría familiarizados con sitios como Google, Ebay, Yahoo y Amazon, pero su popularidad no durara para siempre, así podemos afirmar que sitios como YouTube, MySpace, Bebo, Hi5 y demás páginas comunitarias donde los usuarios pueden intercambiar contenidos serán el foco para las comunidades *online* durante el 2007, esto aunado al crecimiento en la utilización de la telefonía celular en aplicaciones de Internet, ya que dicha tecnología nos permite tener videoconferencias en tiempo real, correo electrónico y acceso a Internet casi en cualquier lugar.
- "La historia de la tecnología es también la historia de la invasión de la vida privada" (Mark Lemley)
- La cuenta de correo electrónico debe ser considerada como un dato de carácter personal y tener la protección de los datos considerados como tales, en los países donde este legislado.

- 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.
- La creación de un sistema de seguridad criptográfico es la solución más viable 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.
- 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* como el "correo basura" que, por lo general. No tiene carácter comercial y que suele provenir de direcciones no anónimas. El llamado *spam* o bombardeo publicitario se define tradicionalmente como "los mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas.
- Se 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 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.
- Una solución para evitar el correo no deseado es 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.
- Otra solución presentada para este problema es la inclusión de filtros en los servidores, por medio de los cuales se detectaría y se imposibilitaría el ingreso de correos no solicitado. 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 embargo, 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.
- La situación en nuestro país al decir de la doctrina existente, es la de contar con un sistema de listas de exclusión (*opt-out*) según lo señala el artículo 18 de la Ley Federal de Protección al Consumidor, que se refiere a que la Procuraduría Federal de Protección al Consumidor pueda llevar un registro público que será gratuito, de consumidores que no deseen que su información sea utilizada con fines publicitarios, quienes podrían

comunicar a la PROFECO su solicitud de inscripción en este registro, además el artículo 18 bis del mismo ordenamiento prohíbe a los proveedores y empresas el envió de publicidad a los consumidores que expresamente les hayan manifestado su voluntad de no recibirla o que estén inscritos en el registro del artículo 18.

- Se definen tradicionalmente como *cookie* (espía, cukie, caqui, fisgón, galletita) a los ficheros de datos guardados en un directorio específico del ordenador del usuario. Se crean por los servidores *web* con el objeto de ser enviados a los programas navegadores del usuario, y así recoger la información de que dicho fichero ha reunido. Por lo tanto son considerados como datos personales.
- 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 página *web*, consultoría de diseño e implantación de *webs* e Internet, etc.,)".
- La solución está en que los proveedores de servicio de Internet instalen programa filtro en la red que impida el acceso a sitios *web* ilegales. Otra solución y tal vez más factible es la autorregulación, o la firma de Tratados Internacionales que legislen sobre el tema.
- No son tan efectivas las políticas de seguridad que los sitios *web* ofrecen y éstos atetan muchas veces contra el derecho a la vida privada de las personas sin que siquiera nos percatemos de ello.
- El caso más alarmante 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, CURP, IFE, cédula profesional, estado civil, etcétera.
- En la actualidad existe un fenómeno en la red respecto del impacto que produce en la vida privada de las personas en relación a la amenaza que se ha vuelto este medio de comunicación a la hora de controlar a los empleados.
- 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?
- En nuestro país no existe una regulación específica ni precedente alguno en jurisprudencia sobre el uso del correo electrónico e Internet en las relaciones laborales, la única disposición que existe es el artículo 135 de la Ley Federal del Trabajo que en su fracción IX, señala que el trabajador tiene la obligación de utilizar las herramientas de trabajo únicamente para el objeto para el que le fueron destinadas, por lo que se puede concluir que actuar en contra de lo que señala este numeral puede significar una causa de rescisión de contrato de trabajo sin responsabilidad alguna para el empleador.

- Es necesario hacer respetar las reglas relativas a la protección de la vida privada y el secreto de correspondencias en el trabajo, el empresario o patrón no tiene el derecho de interceptar el correo electrónico de sus trabajadores, ya que puede tener una responsabilidad penal por abrir el correo de sus trabajadores.
- La red se ha convertido en un recurso útil para los gobiernos para combatir el terrorismo, pero a la vez en esta labor violentan la vida privada de las personas.
- Es nuestro país para garantizar la presencia de la autoridad en la supercarretera de la información, la Policía Federal Preventiva desarrolló en México la primera Unidad de Policía Cibernética, que además de las acciones preventivas en materia de delitos cometidos en Internet y usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra menores, como existen en los países desarrollados.
- Surge 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.
- "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". (Hernán Corral)
- Existen dos tipos de soluciones a la violación a la vida privada en Internet unas de tipo técnico y otras jurídicas.
- Dentro de las técnicas, el proyecto P3P consiste en que 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 cundo se conecte a un sitio *web*. El agente de usuario puede residir en el propio ordenador del usuario o en el del proveedor de servicio. Es 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) 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.
- La adopción del sistema opt-in, que se trata de un sistema que requiere 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. 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.
- Otra solución técnica es el sistema *TRUSTe* 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.

- Los certificados de garantía, 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".
- Otra solución tecnológica es la implementación de los programas filtro que tienen por objeto filtrar aquellos contenidos que sean ilícitos o no deseados por el usuario mientras éste transita en el ciberespacio.
- Dentro de las soluciones jurídicas encontramos, los códigos de conduta llamados también "Códigos Deontológicos", que han sido aplicados en distintos ordenamiento jurídicos europeos. 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 la particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva".
- Otra solución es la autorregulación de la red, a lo cual yo manifiesto que 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 de datos de carácter personal son muy cotizados en el ciberespacio, por lo que pierde viabilidad como solución.
- La solución Safe Harbor, 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".
- La creación de un organismo internacional es 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, esta solución no es una alternativa utópica, ya que si bien Internet se caracteriza por no tener un gobierno determinado y ser aterritorial, podría tratarse de un organismo que establezca cuales son las directrices por las que los Internautas deben guiarse al navegar en la red.
- Aplicar el Teorema de Coase, que Como consecuencias de ello, las medidas a tomar por parte de México serían las siguientes:

  3. 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.

4. Aclarar la asignación de los derechos, obligaciones y responsabilidades de quienes son sujetos activos o pasivos en el uso de Internet, determinando así el rol que cada uno de ellos tiene.

a. La creación de una autoridad interna encargada de la protección de datos, en específico los que obran en manos de particulares. Como ejemplos del modelo europeo tenemos la Agencia Española de Protección de Datos Personales.
b. La mayoría de las Constituciones de los Estados Latinoamericanos garantizan el derecho a la intimidad y privacidad y, explícita o implícitamente, la protección de los datos personales; pero carecen de leyes especiales en la materia, salvo en algunos casos excepcionales. Esto ha propiciado que una gran parte de los propios Estados Latinoamericanos no dispongan de autoridades que tengan como cometido sustantivo y especial el control de datos personales.
c. El modelo de los Estados Unidos de América de protección de la vida privada de las personas se caracteriza por la creciente aparición de normas, en gran medida como consecuencia de la autorregulación y de criterios desarrollados por la propia industria, tendentes a garantizar un mayor respeto a al intimidad de los usuarios
d. 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.

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. Dentro de o 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.

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 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 consiente 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 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 Kaiser, 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 este trabajo puede ser corta debido a los constantes desarrollos de la ciencia, no me queda más que decir que la vida privada de la personas también está destinada a desarrollarse y a resguardarse, y es deber del Estado sentar las bases para ello.

FUENTES CONSULTADAS

FUENTES CONSULTADAS

BIBLIOGRAFÍA

- ACOSTA ROMERO, Miguel, ***Nuevo derecho bancario,*** Editorial Porrúa, México, 1995.
- ALEXI, Robert, ***"Los derechos fundamentales en el Estado democrático de derecho",*** en ***Neoconstitucionalismo (s),*** CARBONELL, Miguel (ed.), Madrid, Trotta, 2003.
- ÁLVAREZ GONZÁLEZ DE CASTILLA, Clara Luz, ***Análisis a las reformas de la Ley Federal de Telecomunicaciones*** en ***Reforma de medios electrónicos. ¿Avances o retrocesos?,*** HUBER, Rudolf, VILLANUEVA, Ernesto (coords.) UNAM, Instituto de Investigaciones Jurídicas, 2007.
- ANDRÉS CAMPOLI, Gabriel, ***La firma electrónica en el régimen comercial mexicano,*** Editorial Porrúa, México, 2004.
- AVELEYRA M. Antonio, ***La transición democrática en México, el derecho a la libertad informática, y el derecho a la intimidad,*** México, 2002, http://profesor.sis.uia.mx/aveleyra/comunica/privacidad/tdm.htm
  La comunicación de mensajes de datos personales en México. El predecible estado de arte: la administración pública los desarrollos privados y los esfuerzos legislativos 2003-2004, Derecho Comparado de la Información, No. 4, Julio – Diciembre 2004, Instituto de Investigaciones Jurídicas, UNAM.
- BAJO FERNANDEZ, Miguel, ***"El secreto profesional en el proyecto de Código Penal,"*** en Anuario de Derecho Penal, Madrid, 1980.
- BANINTER, Robert, ***Le drout au respect de la vie privée,*** Jurisclasseur Périodique, 1968,V.I., No. 2136
- BARAN, Paul, ***On Distributed Communications Networks,*** IEEE Trans. Comm Sys. Estados Unidos de América, Marzo de 1962.
- BARRERA María Helena, ***Correspondencia Digital: Recreando Privacidad en el Ciberespacio,*** Revista de Derecho Informático, No.015, octubre de 1999, http://www.alfa-redi.org/rdi-articulo.shtml?x=345
- BATTLE SALES, Georgina, ***Las convenciones ilícitas en los negocios mercantiles,*** Revista de Derecho Mercantil, Universidad La Rioja, No. 205, 1992.
- BELLAMY, Bojana, ***Privacy Laws & Business International Data Protección Roundup,*** Revista Privacy Laws&Bussines, International Newsletter, N°60, enero de 2002.
- BLOUSTEIN, Edward, ***Privacy as dear at any price: a response to profesor Posner' s Economic Theory,*** en Georgia Law Review 12, 1978.
- BRIRCHMAN, A. Jeremy, ***Is P3P "the devil"?,*** University of Miami School of Law, May, 1998, http://personal.law.miami.edu/~froomkin/sem97/birchman.html
- BROSINI, Victtorio, ***Informática y Derecho,*** Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1988.
- BUENROSTRO, CUERVO, GUTIÉRREZ Y ROSADO, ***Los Negocios en Internet hoy y en México,*** Mc Graw Hill, México, 1997.
- CABALLERO JUÁREZ, José Antonio y GREGORIO, Carlos, (editores) ***El acceso a la información Judicial en México: una visión comparada,*** Instituto de Investigaciones Jurídicas UNAM, México, 2005.
- CARBONELL, Miguel, ***El derecho de acceso a la información como derecho fundamental*** en LÓPEZ-AYLLÓN, Sergio (coord.), ***Democracia, transparencia y Constitución: propuestas para un debate necesario,*** México, UNAM, Instituto de Investigaciones Jurídicas, 2006.
  Los derechos fundamentales en México, Instituto de Investigaciones Jurídicas, UNAM, México, 2004.
- CARPIZO, Jorge, ***"Constitución e información",*** en CARBONELL Y VALADES (coords.), ***Constitucionalismo iberoamericano del siglo XXI,*** UNAM, Instituto de Investigaciones Jurídicas, México, 2000.
- CARRASCO ARAIZAGA, Jorge, ***Sahagún contra la pared,*** Semanario Proceso, No. 1578, México, 28 de enero de 2007.
- CARRASCO BLANC, Humberto, ***Algunos Aspectos de la Responsabilidad de los Proveedores de Servicios y Contenidos de Internet. El caso "ENTEL",*** Revista de Derecho Informático, No. 26, septiembre de 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=554
- CASACUBERTA, David, ***La privacidad en los nuevos medios electrónicos. Aspectos éticos y sociales,*** Revista de Derecho Informático, No.011, junio de 1999. http://www.alfa-redi.org/rdi-articulo.shtml?x=276
- CASTILLO MARCANO, José Luis, ***El Derecho a la Intimidad y la Protección de Datos Personales en el Derecho Español,*** Boletín de la Academia de Ciencia Políticas y Sociales. No. 134. Año LXIV, Caracas, 1997.
- CASTRO V, Juventino, ***Garantías y Amparo,*** México, décimo primera edición, Editorial Porrúa, 2000.
- CEA EGAÑA, José, ***Manual de Derecho Constitucional,*** Tomo II, Chile, 1996.
- CELIS QUINTAL, Marcos Alejandro, ***La protección a la intimidad como derecho fundamental de los mexicanos,*** en CIENFUEGOS SALGADO, David y MACIAS VÁZQUEZ, María Carmen (coords.), ***Estudios en homenaje a Marcia Muñoz de Alba Medrano. Protección a la persona y derechos fundamentales,*** México, UNAM, Instituto de Investigaciones Jurídicas, 2006.
- CIENFUEGOS SALGADO, David y MACÍAS VÁZQUEZ, María Carmen, ***Estudios en homenaje a Marcia Muñoz de Alba Medrano Bioderecho, tecnología, salud y derecho genómico,*** Instituto de Investigaciones Jurídicas, UNAM, México, 2006.

- CIFUENTES, Eduardo, ***El habeas data en Colombia***, en Derecho a la autodeterminación informativa y acción de Hábeas Data en Iberoamérica, Revista Ius et Praxis, año 3 No 1, universidad de Talca, Chile, 1997.
- COLLARD, Royer, ***De la Liberté de Resse, (Discours)***, Paris, 1949.
- ***Compilación de normas y criterios en materia de transparencia y acceso a la información pública de la Suprema Corte de Justicia de la Nación***, SCJN, México, 2005.
- CORRAL TALCIANI Hernán, ***Configuración Jurídica del Derecho a la Privacidad II: concepto y delimitación***, Revista Chilena de Derecho, Vol. 27 No. 2, Sección Estudios.
- CRUZ, Patricia, La práctica de la ética en los medios de comunicación, Academia Mexicana de Derechos Humanos, México, 1999.
- CUERVO, José, ***La Intimidación Informática del Trabajador***, Revista de Derecho Informático, No. 003, octubre de 1998, http://www.alfa-redi.org/rdi-articulo.shtml?x=158
- DÁVARA RODRIGUEZ, Miguel Ángel, ***Manual de derecho informático***, Aranzandi Editores, Madrid, España, 1997.
- DAVARA RODRIGUEZ, Miguel Ángel, ***La Ley española de protección de datos (LORTAD):¿una limitación al uso de la informática para garantizar la intimidad?***, Actualidad Jurídica No. 12, Elcano, Aranzandi, 1992.
- DE CUPIS, Adriano, ***Os direitos da personalidade***, Lisboa, 1961.
- DE MIGUEL ASENSIO, Pedro Alberto, ***Derecho del Comercio Electrónico***, Editorial Porrúa, México, 2005.
- DE VERGOTTINI, Giussepe, ***Derecho Constitucional Comparado***, UNAM y Segretariato Europeo per le Pubblicazioni Scientifiche, México, 2006.
- DEL PESO NAVARRO, Emilio, ***Resolución de conflictos en el intercambio electrónico de documentos***, en Ámbito Jurídico de la información, Cuadernos de Derecho Judicial, Escuela Judicial-Consejo General del Poder Judicial, Madrid, 1996
- DIAZ ARIAS, Rafael, ***Transferencia de Datos Personales. ¿Llegarán nuestros datos a buen puerto?***, Revista de Derecho Informático, No. 023, junio de 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=488
- DOGLIOTTI, Massimo. ***Il diritto alla riservatezza in Italia e in Francia: orientamenti dottrinali e giurisprudenziali***, o BESSONE y GIACOBBE (Eds.) ***Il diritto alla riservatezza in Italia ed in Francia***. Cedam, Padua 1988.
- EKMEKDIJAN Miguel A y PIZZOLO, Calogero, ***Hábeas data. El derecho a la intimidad frente a la revolución informática***, Depalma, Buenos Aires, 1996.
- ***Encuesta Nacional sobre Disponibilidad y Uso de Tecnología de Información*** ,INEGI, México, 2004.
- ESCALANTE GONZALBO, Fernando, ***El Derecho a la privacidad***, Cuadernos de Transparencia 02, IFAI, México, 2004.
- ESTADELLA YUSTE, Olga ***"La Protección de la Intimidad frente a la Transmisión Internacional de Datos Personales"*** Centre d'Investigació de la Comunicació, Generalitat de Catalunya. Editorial Tecnos. Madrid, 1995.
- EVANS DE LA CUADRA, Enrique, ***Los Derechos Constitucionales, Tomo 1***, Editorial Jurídica de Chile, Santiago, 1986.
- FERRAJOLI, Luigi, ***Derechos y garantías. La ley del más débil***, Editorial Trotta, Madrid, 2004.
  El garantismo y la filosofía del derecho, Universidad externado de Colombia, Bogotá, 2000.
- FERREYRA, Gonzalo C, ***Internet paso a paso: Hacia la autopista de la información***, Grupo Editor Alfaomega, México, 1996..
- FILHO, Democrito. R, ***Short commentaries on the CAN-SPAM Act***, Revista de Derecho Informático, No. 70, mayo del 2004, http://www.alfa-redi.org/rdi-articulo.shtml?x=1093
- FLORES TREJO, Fernando, ***Bioderecho***, Editorial Porrúa, México, 2004.
- FRASER, Barry, ***Rules of the Road Navigating the Information Superhighway***, Human Rights Magazine, Volume 26, No 1, 1999. http://www.abanet.org/irr/hr/winter99_fraser.html
- GALLOUEDEC- GENUYS, Francoise & LEMOINE, Philippe, ***La informatización: riesgos culturales***, Barcelona, Mitre.
- GARCÍA GONZALEZ, Aristeo, La ***Protección de Datos Personales, Derecho Fundamental del Siglo XXI***. Un Estudio Comparado. Revista de Derecho Informático, No. 100, Noviembre de 2006, http://www.alfa-redi.org/rdi-articulo.shtml?x=7851
- GARCÍA SAN MIGUEL, Luis, ***Estudios sobre el derecho a la intimidad***, Editorial Tecnos, Madrid, 1992.
- GARZÓN VALDÉS, Ernesto, ***Lo íntimo, lo privado y lo público***, Cuadernos de Transparencia 06, IFAI, México, 2005.
- GIRALDO QUINTERO, Argiro, ***El Secreto en la Comunicación por Correo Electrónico***, Revista Electrónica de Derecho Informático, Número 025, agosto del 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=539
- GOMEZ ROBLEDO, Alonso y ORNELAS NUÑEZ, Lina, ***Protección de datos personales en México: el caso del Poder Ejecutivo Federal***, Instituto de Investigaciones Jurídicas, UNAM, México, 2006.
- GONZALEZ GAITANO, Norberto, ***El deber de respeto a la intimidad: información pública y relación social***, Ediciones Universidad de Navarra, Pamplona, 1990.
- GOOD, Edgar, ***An email Education. What You D'ont Know About Email Can and Will Hurt You***, International Journal of Communications Law and Policy, Oxford University, U.K. 1999.
- GUERRERO AMPARÁN, Juan Pablo, ***Nueva tecnologías en materia de acceso a la información y protección de datos personales***, Suprema Corte de Justicia de la Nación, http://200.38.86.53/NR/rdonlyres/178A09DC-CE5B-4AD6-AFB6-62ECAD9D3F8D/0/IFAIJPGADPTecnologias26sep06ppt.pdf
- H. GATES, William, ***Ensayo para el Presidente de Estados Unidos George W. Bush. Moldeando la era Internet***, Diario El Mercurio, 8 de febrero de 2000, pág. 16. Su versión online en Diario de la Sociedad Civil, http://www.sociedadcivil.cl/nuevodiario/sitio/Informaciones/documento.asp?Id=127

- HERRÁN ORTIZ, Ana Isabel, ***La violación de la intimidad en la protección de datos personales***, Editorial Dykinson, Madrid, 1998.

  El derecho a la protección de datos personales en la sociedad de la información, Universidad de Deusto, Bilbao, España, 2003.
- HERRERA BRAVO, Rodolfo y HERNANDEZ RUBIO, Montserrat, ***La Legitimidad del Control Tecnológico del Empleador sobre al Trabajador***, Revista de Derecho Informático, No. 035, junio de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=709
- Instituto Nacional de Estadística e Informática, ***Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares***, Usuarios de Internet por genero, 2001 a 2006. http://www.inegi.gob.mx/est/contenidos/espanol/rutinas/ept.asp?t=tinf216&c=5565
- JIJENA LEIVA, Renato, ***Responsabilidad de los ISP por la difusión de contenidos* online**, Revista Electrónica de Derecho Informático, No. 15, octubre de 1999, http://premium.vlex.com/doctrina/REDI-Revista-Electronica-Derecho-Informatico/Informe-legal-Improcedencia-consurar-legalmente-contenidos-Internet-Analisis-Boletin-N%B02395-19/2100-107405,01.html

  Chile, la protección penal de la intimidad y el delito informático, Editorial Jurídica de Chile, Santiago, 1992.

  La nueva ley chilena de protección de datos personales, No.19.628 del 28 de agosto de 1999, Informe legal.
- JIMENEZ GUZMÁN, Luis, ***Hacia una regulación del Comercio electrónico en México***, Tesis Profesional, México, 2000.
- KAISER, Pierre, ***La protección de la vie privée, Presses Universitaires d´Aix- Marseille***, 2e Edition, 1990.
- KLEINROCK, L., ***Information Flow in Large Communications Nets***, RLE Quarterly Progress Report, Estados Unidos de America, Julio de 1961.
- LA SAGRADA BIBLIA, ***Mateo 20***, Royce Editores, México, 2004.
- LAU, Stepehn, ***Comercio electrónico, derecho del consumidor y protección de datos***, Memorias de la XX Conferencia Internacional de Autoridades de Protección de Datos, Santiago de Compostela, España, 1998
- LEMLEY, Mark, ***Software and Internet Law***, Aspen Publishers New York, NY, 2003.
- LEÓN, Carlos Alfredo en ***Consideraciones Legales Relativas al Envío de emails. Comerciales No Solicitados***, dicho texto publicado en Revista de Derecho Informático, Número 036, julio de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=730
- LICKLIDER, J.C.R., y W. CLARK, ***On- Line Man-Computer Communication, Agosto 1962 en Proceeding of the IEEE***, Edición especial de Comunicacónes de redes mediante paquetes, volúmen 66, Nº 11, Estados Unidos de Amórica, Enero 1972.
- LLANEZA GONZÁLEZ, Paloma, ***Internet y Comunicaciones Digitales***, Editorial Bosch, Barcelona, España 2000.
- LUCAS MURILLO DE LA CUEVA, Pablo, ***El derecho a la autodeterminación informativa***, Editorial Tecnos, Madrid, 1990.
- LUSKY, Louis, ***Invasion of Privacy: A Clarification of Concepts***, Political Science Quarterly,Vol.87, No.2,, junio de 1972.
- MANTONI, Luis María, en ***El derecho a la intimidad***, Editorial Trivium. Madrid, 1983.
- MARTÍN, Lucien, ***Le secret de la vie privée, Revue Trimestrelle de Droit Civil***, LVII, T, 57, an 1959.
- MÉJAN, Luis Manuel, ***El secreto bancario***, Biblioteca FELABAN, Bogotá Colombia, 1994.
- MEJIA, Marcelo, BARRERA, Alejandra y KULHMANN, Federico, ***Introducción a las tecnologías de la información y de las comunicaciones (TICS) y a su aplicación en los negocios electrónicos***, en NAVRRO ISLA, Jorge (coord), ***Tecnologías de la Información y de las comunicaciones: Aspectos legales***, Editorial Porrúa e ITAM, México, 2005.
- MENDOZA LUNA, Amilcar, ***Los Cookies ¿amenaza a la privacidad de información en la Internet?,*** Revista de Derecho Informático, No. 031, enero de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=612
- MOEYKENS Rafael Federico y SALTOR Carlos Eduardo, en Argentina: ***La protección de Datos Personales en el Proyecto de Códigos Civil unificado de la República Argentina***, Revista Electrónica de Derecho Informático. Número 023, junio de 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=486
- MUÑOZ DE ALBA MEDRANO, Marcia, **Habeas Data** en ***Estudios en homenaje a Marcia Muñoz de Alba Medrano. Estudios de Derecho Público y Política***, CIENFUEGOS SALGADO, David y MACÍAS VAZQUEZ, María del Carmen (coords.) UNAM, Instituto de Investigaciones Jurídicas, México, 2006.
- NOVOA MONREAL, Eduardo, ***Derecho a la vida privada y Libertad de Información***, Siglo XXI Editores SA. de CV, México D.F., cuarta edición, 1989.
- NÚÑEZ PONCE, Julio, ***La acción constitucional de Habeas Datas y la comercialización de información judicial***, Revista de Derecho Informático, No. 13, Agosto de 1999, http://www.alfa-redi.org/rdi-articulo.shtml?x=316
- OCHOA OLVERA, Salvador, ***La demanda por Daño Moral***, Montealto Editores, México, 1999.

  Protección civil del honor, Editorial Porrúa, México, 2006.
- OVILLA BUENO, Rocío, ***La protección jurídica de las bases de datos en México. De los lineamientos internacionales a la Nueva Ley Federal del Derecho de Autor*** en ***Estudios de Derecho Intelectual en homenaje a David Medina Rangel***, Becerra Ramírez Manuel (compilador), UNAM, Instituto de Investigaciones Jurídicas, México, 1998.

  La protección de los datos personales en México, Editorial Porrúa, México, 2005, Colección Breviarios Jurídicos No. 28.
- PARKER, Richard, ***A definition of privacy***, Rutger´s Law Review, No 27, 1974.
- PECES-BARBA, G. ***Curso de derechos Fundamentales. Teoría general***. BOE, Madrid, 1999-

- PEÑA C, ***Sistema Jurídico y Derechos Humanos***, Cuaderno de Análisis Jurídico, Universidad Diego Portales, 1996.
- PÉREZ LUÑO, Antonio (director de la edición), ***Problemas actuales de la documentación y la informática jurídica***, en capítulo escrito por DENNINGER, Erhard, pág. 271, Editorial Tecnos S.A., Madrid, 1987.
- 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.

  De/ habeas corpus a/ habeas data, Editorial Aranzadi, Madrid, 1991.

  Dilemas actuales de la protección de la intimidad. Revista Ius et Praxis Universidad de Lima. Perú, 1992, Nº 21-22.

  Los derechos humanos en la sociedad tecnológica en Cuadernos y debates, Editorial Centro de Estudios Constitucionales, Madrid, 1989.
- PLASENCIA VILLANUEVA, Raúl, ***Ley Federal contra la Delincuencia Organizada*** en ***Anuario Jurídico 1996***, UNAM, Instituto de Investigaciones Jurídicas.
- POMEROY, Jeremy en ***Online Anonymity can be Illusory Under Current Law, ISP Policies*** Multimedia & Web Strategist, Sept. 1998.
- POSNER, Richard, ***The Right of Privacy***, en Georgia Law Review, 12(3), 1978.
- PUCCINELLI, Oscar, ***El Habeas Data en Indoiberoamérica***, Editorial Temis S.A., Santa Fe de Bogotá, Colombia, 1999.
- PUENTE ESCOBAR, Agustín, "Breve descripción de la evolución histórica del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal", ***Protección de datos de carácter personal en Iberoamérica,*** Agencia Española de Protección de Datos, 2005.
- QUINTANA VALTIERRA, Jesús y CARREÑO GARCÍA, Franco, ***Derecho Parlamentario y Técnica Legislativa en México***, Editorial Porrúa, México, 2006.
- QUINTANA, J, ***Multimèdia: què i per a què***, Revista Guix, núm. 233, Paris, 1997.
- QUIROGA LAVIÉ, Humberto, ***La protección de la intimidad y la regulación del secreto*** en ***Derecho a la información y derechos humanos***, CARPIZO, Jorge y CARBONELL, Miguel (coords.) UNAM, Instituto de Investigaciones Jurídicas, México, 2000, pág. 503.
- R. GIESZE, Craig, ***El análisis económico de la información privilegiada en el mercado de capitales y valores:¿Justicia ineficiente?,*** Revista Chilena de Derecho, Vol.26 No 4, Chile, 1999.
- RAMIREZ CHELALA, Yesín y VERA PRENDES, Luis, ***Aspectos Laborales de la sociedad de la información*** en NAVARRO ISLA, Jorge, (coord) ***Tecnologías de la Información y de las comunicaciones aspectos legales***, Editorial Porrúa, México, 2005.
- RAMÍREZ RAMÍREZ, Agustín, ***Tratamiento jurídico de los datos clínicos en México (Información y límites de acceso)*** en CIENFUEGOS SALGADO, David y MACIAS VAZQUEZ, María Carmén (coords) ***Estudios en homenaje a Marcia Muñoz de Alba Medrano. Bioderecho, Tecnología, Salud y Derecho Génomico,*** Instituto de Investigaciones Jurídicas, UNAM, 2006.
- REYES KRAFFT, Alfredo, ***La firma electrónica y las entidades de certificación***, Editorial Porrúa, México, 2003

  Protección de Datos Personales en México. Génesis Legislativa, Revista de Derecho Informático, No. 100, Noviembre 2006, http://www.alfa-redi.org/rdi-articulo.shtml?x=7846
- RÍOS ESTAVILLO, Juan José, ***Derecho a la información en México***, Editorial Porrúa, México, 2005.
- ROBERTO SOBRINO, Waldo Augusto, ***Las "Cookies" y el "Spam" (y la violación de la "Privacidad" y la "Intimidad")***.Revista de Derecho Informático No.035 de junio de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=710
- ROBERTS,L., ***Multiple Computer Networks and Intercomputer Communications;*** Conferencia de la Association for Computer Machinery en Gatlinburg, Octubre de 1967.
- ROJAS AMANDI, Víctor Manuel, ***El uso de Internet en el derecho***, Oxford University Press, México, 2001.
- ROSEMBERG HOLCBLAT Alexander y SÁNCHEZ SANZ Moriah, ***El derecho a la privacidad en Internet,*** Revista de Derecho Informático, No.37, Agosto de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=770
- RUBIO DE MEDINA, María Dolores, ***El despido por utilización personal del correo electrónico***, Editorial Bosch, España, 2003.
- S ELIAS, Miguel, ***Situación Legal de los Datos de Carácter Personal frente a las Nuevas Tecnologías,*** Revista de Derecho Informático, No. 032, marzo de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=638
- SALGADO PESANTEZ, Hernán, ***Lecciones de Derecho Constitucional***, Ediciones Legales, Quito, Ecuador, 2004.
- SÁNCHEZ ALMEIDA, Carlos, ***Intimidad: Un derecho en Crisis. La Erosión de la Privacidad***, Revista de Derecho Informático, No. 024, julio del 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=504
- SÁNCHEZ BRAVO, Álvaro, ***La protección del derecho a la libertad informática en la Unión Europea,*** Universidad de Sevilla, Secretariado de Publicaciones. Sevilla – España. 1998.
- SANCHEZ BRINGAS, Enrique, ***Derecho Constitucional***, Editorial Porrúa, México, 2006.
- SEBAG-MONTEFIORE, Hugh, ***Enigma: The battle for the code,*** Published by Jhon Wiley & Sons, Hoboken, New Jersey, 2000.
- SMEDINGHOFF, Thomas J. ***On-line Law.*** Addison-Wesley Developers Press, United States of America, 2000.
- STONE, Brad, ***Spam Doubles, Finding New Ways to Deliver Itself*** *New York Times*, 6 de diciembre de 2006.
- SUÑE LLINÁS, Emilio, ***Tratado de Derecho Informático, Vol. I***, Universidad Complutense, Madrid-España. 2000.
- TAN, Koon. ***Phishing and Spamming via IM (SPIM).*** Internet Storm Center, 5 de diciembre del 2006
- TELLEZ VALDEZ, Julio, ***Derecho Informático***, McGraw – Hill, México, 2004, págs. 59-60.

- ***Transparencia, acceso a la información y datos personales. Marco Normativo***, Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, IFAI, México, 2004.
- URABAYEN, Miguel, ***Vida Privada e Información: un conflicto permanente***, Pamplona, Ediciones Universidad de Navarra.
- URIOSTE, Mercedes, ***Protección de Datos Personales***, Investigaciones 1, Subsecretaría de Investigación en derecho comparado de la CSJN, Buenos Aries, Argentina, 1998.
- V.G. CERF y R. E. KAHN, ***"A Protocol for packet Network Interconnection"***, IEEE Trans. Comm. Tech., Vol. Com-22, V5, Estados Unidos de América, Mayo de 1974.
- VALLEPUGA GONZÁLEZ, Paula ***Responsabilidad de los Prestadores de Servicio en la Sociedad de la Información***, Revista de Derecho Informático, No. 030, enero de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=615
- VILLANUEVA, Ernesto, ***Derecho de acceso a la comunicación pública en Latinoamérica***, Estudio Introductoria y compilación, Instituto de Investigaciones Jurídicas, UNAM, México, 2003.

  Derecho de la Información, H. Cámara de Diputados-Miguel Angél Porrúa Editor, México, 2006.

  Derecho mexicano de la Información, Oxford, México, 2000.
- VILLATE, Javier, P3P, ***un estándar para la privacidad, ¿ Es lo que necesitamos?***, Revista de Derecho Informático, No. 001, agosto de 1998, http://www.alfa-redi.org/rdi-articulo.shtml?x=138
- VIÑAMANTA PASCHKES, Carlos, ***Indigenismo y Propiedad Intelectual***, Editorial Porrúa, México, 2006.
- VIVANCO, Ángela. ***Las libertades de Opinión y de Información***, Editorial Andrés Bello, Santiago, 1992.
- WARREN, Samuel y BRANDEIS, Louis, ***El derecho a la Intimidad***, Editorial Civitas, Madrid, 1995, Introducción de PENDÁS, Benigno.
- WESTIN, Alan F. ***Privacy and Freedom***, N.Y. Atheneum, New York, 1967.
- ZWEIGERT, Konrad y KÖTZ, Hein, ***Introducción al Estudio del Derecho Comparado***, Oxford Universty Press, México, 2002.

DICCIONARIOS Y ENCICLOPEDIAS

- ***Black´s Law Dictionary***, The Publishers Editorial Staff, St. Paul Minn, West Publishing Co, 1979.
- BURGOA ORIHUELA, Ignacio, ***Diccionario de Derecho Constitucional, Garantías y Amparo***, Editorial Porrúa, México, 2005.
- CABANELLAS DE LAS CUEVAS Guillermo y C.HOAGUE, Eleanor, ***Law Dictionary***, Tomo 1 English-Spanish, Editorial Heliasta, Buenos Aries, Argentina, 1998.
- ***Diccionario de la Lengua Española***, Real Academia Española, Vigésima Primera Edición, Madrid, 1992.
- ***Diccionario Jurídico Mexicano***, Instituto de Investigaciones Jurídicas UNAM, México, 1996.
- ***Enciclopedia Encarta 2007, disponible en CD-Rom.***
- ***Enciclopedia Jurídica Omeba***, Editorial Bibliográfica Argentina, S.R. L., Buenos Aires, 1962.
- ***Wikipedia, La enciclopedia libre***, http://es.wikipedia.org/

HEMEROGRAFÍA

- ***Clarín*** de fecha de diciembre de 2001, en entrevista al Juez del estado de Minnesota, James M. ROSENBAUM, en un artículo titulado"Ante todo, privacidad".
- CHAVEZ, José Antonio, ***La @ omnipresente***, en ***Reforma*** sección Interfase, Lunes 30 de agosto de 1999.
- DOUGHERTY, Jay, ***¿Cómo hallar una aguja en un pajar?***, Reforma sección Interfase, Lunes 30 de agosto de 1999.
- Elmundo.es, ***"Decisión de los ministros de telecomunicaciones. La UE respetará la privacidad de datos en Internet salvo cuando afecten a la seguridad"***, para acceder directamente a este artículo, remitirse a http://www.elmundo.es/navegante/2001/12/07/seguridad/1007715325.hml, de fecha 7 de diciembre de 2001,
- Elmundo.es, ***La agencia de protección de datos multa a Terra***, 28 de marzo de 2001.
- Elmundo.es, "***La Fiscalía entiende que no es delito que los jefes controlen los emails de sus empleados***" http://www.elmundo.es/navegante/2001/11/26/esociedad/1006801495.html de fecha 26 de noviembre de 2001.
- El País, ***Passport almacena los datos de 150 millones de usuarios***, 25 de octubre de 2000.
- El Universal, ***Multa millonaria a vendedores del padrón electoral***, en su edición del día, sábado 16 de diciembre de 2006. http://www.eluniversal.com.mx/notas/394453.html
- ***Entrevista a Alejandro Pissanty por Ernesto López***, Reforma, Sección Interfase, México, lunes 13 de julio de 1998, pág 5A.
- **Hackers *hacen de las suyas en* site *de Cámara de Diputados***, Reforma Sección Interfase, Lunes 22 de febrero de 1999, pág 7A.
- HERNÁNDEZ, Luis Antonio ***"La reforma al Código Penal, apenas un avance"*** en su columna *"Internet y Legislación"*, Lunes 3 de mayo de 1999, *El Universal*, sección *Universo de la Computación*.
- HERNANDEZ, Luis Guillermo, ***El vigilante que todo lo ve y lo oye***, "El Centro"; México, lunes 5 de marzo de 2007.

  También husmea el FBI, "El Centro", México, martes 6 de marzo de 2007.
- MELO DE RAZO, José E. ***Tenga un e-mail alterno***, El Universal, Universo de la Computación, Lunes 21 de junio de 1999, pág 4.
- LÓPEZ, Eduardo, ***Correo electrónico y abuso***, Sección Interfase, Diario Reforma, México, 15 de mayo de 2006.

- LOPEZ, Ernesto, ***De 40 años, y sigue joven***, Reforma, Sección Interfase, México, Lunes 12 de Octubre de 1998. Primera columna.
- ***Todavía es muy masculina***, Diario Reforma, Suplemento especial Internet en la Vida Cotidiana, México, Noviembre 12 de 1998, pág.10.
- ***Los socialistas franceses denuncian un correo falso en su nombre***, Nota publicada en http://delitosinformaticos.com/noticias/101761230840490.shtml, abril del 2002.
- ***New Hotmail breach reported***, 14 de septiembre de 1999, http://www.cnn.com/TECH/computing/9909/14/hotmail/index.html
- NOTIMEX, ***Arranca tarjeta CURP electrónica***, El Economista, México, 1 de agosto de 2006.
- PISANTY, Alejandro y CELORIO, Mariana, ***.MX, Domicilio conocido en Internet***, Revista Entérate en línea, DGSCA, UNAM, México, Mayo de 2002, http://www.enterate.unam.mx/Articulos/2002/mayo/mx.htm
- ***Revista Cuenta y Razón del pensamiento actual***, Entrevista con Anna Birulés, Ministra de Ciencia y Tecnología, No. 117, La Rioja, España, 2000.
- SANCHEZ, Verónica, ***Prevén mayor integración empresarial y menores costos y mejor calidad***, Reforma, Sección Interfase, México, Lunes 12 de Octubre de 1998. Página 13A.
- SAÚL, Lilia, ***Destraban la ley de datos personales***, El Universal, Sección: México, viernes 21 de abril de 2006.
- ***Una Historia que Contar MEXNET A.C.***, ISOC México, www.isoc.com.mx y ***Revista NET@***, Vol 1, Num 19,México,1997.
- WAYNER, Meter ***Abren "portales" a la Red***, Reforma sección Interfase, Lunes 13 de Julio de 1998.

INICIATIVAS, DICTAMENES Y DOCUMENTOS LEGISLATIVOS

- ***Dictamen en sentido negativo, de la Minuta con Proyecto de Decreto por el que se expide la Ley Federal de Protección de Datos Personales***, Agencia Española de Protección de Datos Personales, 14 de diciembre 2005, https://www.agpd.es/upload/Canal_Documentacion/legislacion/Dictamen%20retirada%20Ley%20Mexicana.pdf
- ***Exposición de motivos de la Iniciativa que contiene el proyecto de decreto que reforma el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos***, Gaceta Parlamentaria, No. 164, 2006, del Miércoles 5 de abril de 2006.
- Gaceta del Senado, No. 101, Año. 2007, México D.F., martes 24 de abril, Senado de la República, **Dictamen de las Comisiones Unidas de Puntos Constitucionales; y de Estudios Legislativos, segunda, el que contiene proyecto de decreto que adiciona un segundo párrafo al artículo 6 de la Constitución Política de los Estados Unidos Mexicanos,** http://www.senado.gob.mx/sgsp/gaceta/?sesion=2007/04/24/1&documento=62
- Gaceta del Senado, No. 14, Año. 2006, México D.F., miércoles 9 de agosto, Senado de la República, ***Iniciativa del Senador José Alberto Castañeda Pérez del grupo parlamentario del Partido Acción Nacional que contiene proyecto de Decreto que reforma el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos,*** http://www.senado.gob.mx/sgsp/gaceta/index2.php?sesion=2006/08/09/1&documento=23
- Gaceta del Senado, No. 166, Año. 2006, México D.F., martes 18 de abril, Senado de la República, ***Dictamen de las Comisiones unidas de Puntos Constitucionales y Estudios Legislativos, el que contiene el proyecto de decreto por el cual se adicionan dos párrafos al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos,*** http://www.senado.gob.mx/sen60/sgsp/gaceta/?sesion=2006/04/18/1&documento=36
- ***Gaceta del Senado, No.164, Año 2006***, México, D.F., miércoles 5 de abril de 2006, Senado de la República, http://www.senado.gob.mx/sgsp/gaceta/index2.php?sesion=2006/04/05/1&documento=9
- Gaceta Parlamentaria Año III, No. 474 miércoles 22 de marzo de 2000, ***Proyecto de Iniciativa de Ley que Reforma y Adiciona Diversas Disposiciones del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal, con objeto de penalizar lo referente a delitos informáticos***, http://gaceta.diputados.gob.mx/Gaceta/2000/mar/20000322.html
- Gaceta Parlamentaria año IV, No. 688 de jueves 15 de febrero de 2002, Cámara de Diputados, México, D.F. 2002 ***Iniciativa de Ley Federal de Protección de Datos Personales, presentada por el Senador Antonio García Torres del Grupo Parlamentario del Partido Revolucionario Institucional, en la Sesión de la Comisión Permanente del Miércoles 14 de febrero de 2002,*** http://gaceta.diputados.gob.mx/Gaceta/58/2001/feb/20010215.html#Ini20010215AntonioGarcia
- ***Gaceta Parlamentaria, año IV, número 692***, Cámara de Diputados, México, D.F., miércoles 21 de febrero de 2001, http://gaceta.diputados.gob.mx/Gaceta/58/2001/feb/20010221.html#Ini20010221Antonio
- ***Gaceta Parlamentaria, año IX, número 2021***, Cámara de Diputados, México, D.F., lunes 5 de junio de 2006, http://gaceta.diputados.gob.mx/
- Gaceta Parlamentaria, No. 1895-1, Año. 2005, México D.F. jueves 1º de diciembre, Cámara de Diputados, ***Iniciativa de Ley Federal de Protección de Datos Personales, presentada por el diputado Jesús Martínez Álvarez del Partido Convergencia, el 1º de diciembre de 2005*** http://gaceta.diputados.gob.mx/Gaceta/59/2005/dic/Anexo-I-01dic.html
- Gaceta Parlamentaria, núm. 1953-I, jueves 23 de febrero de 2006, Cámara de Diputados, México D.F., ***Iniciativa de Ley Federal de Protección de Datos Personales, presentada por el Diputado David Hernández del Partido Revolucionario Institucional, el 23 de febrero de 2006,*** http://gaceta.diputados.gob.mx/
- ***Iniciativa de adición al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, presentada por el Senador Antonio García Torres (PRI), el 5 de abril de 2006***, Gaceta

Parlamentaria, No. 164, http://www.senado.gob.mx/sen60/sgsp/gaceta/?sesion=2006/04/05/1&documento=9

- ***Versión estenográfica de la Sesión Pública Ordinaria de la Cámara de Senadores celebrada el jueves 2 de febrero de 2006***, Servicios Legislativos de la Cámara de Senadores, México, D.F. disponible en línea: http://www.senado.gob.mx/servicios_parlamentarios.php?ver=estenografia&tipo=O&a=2006&m=02&d=02

LEGISLACIÓN INTERNACIONAL

- Asamblea General de la Organización de las Naciones Unidas, ***Convención Sobre los Derechos del Niño***, celebrada con fecha 29 de enero de 1991.
- 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.
- ***Aviation and Transportation Security Act***, Transportation and Security Administration of The United States of America (TSA), http://www.tsa.gov/research/laws/law_regulation_rule_0010.shtm
- ***Código Civil de la República de Francia***. Código traducido en la siguiente página: http://www.legifrance.gouv.fr/html/codes_traduits/somcives.htm
- Consejo de Europa, ***Convención Europea de Derechos Humanos***, 3 de septiembre de 1953.
- Consejo Ejecutivo de la Generalidad de Cataluña, el Defensor del Pueblo, el Parlamento de Cataluña y 56 Diputados contra determinados artículos de la Ley 5/1992 de 29 de Octubre, de Regulación el Tratamiento Automatizado de Datos de Carácter Personal.
- Constitución de la República Federativa de Brasil. ***Cámara de Diputados de la República Federativa de Brasil***, http://www2.camara.gov.br/legislacao/constituicaofederal.html
- ***Constitución de la República Italiana***, de la página web de la Corte constituzionale della Repubblica italiana, http://www.cortecostituzionale.it/esl/testinormativi/costituzionedellarepubblica/costituzione_parte_I.asp
- Constitución de Weimar de 1919, traducción del Profesor Benito Aláez Corral, disponible *online*: http://hc.rediris.es/05/constituciones/html/ca1919.htm
- ***Constitución Española aprobada por las Cortes en Sesiones Plenarias del Congreso de los Diputados y del Senado.*** 31 de Octubre de 1978. Raficada 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
- Constitución Federal de la República Argentina, ***Honorable Senado de la Nación***, http://www.senado.gov.ar/web/intores/constitucion/capitulo2.php
- Constitución Política de la República del Ecuador, ***Gobierno Nacional de la República de Ecuador***, http://www.presidencia.gov.ec/modulos.asp?id=109
- ***Data Protection Act***, Public Sector Information United Kingdom, http://www.opsi.gov.uk/acts/acts1998/19980029.htm
- ***Federal Data Protection Act*** o en alemán ***Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung***, del 20 de diciembre de 1990. República ded Alemania. http://www.iuscomp.org/gla/statutes/BDSG.htm
- ***Declaración de los Derechos del Hombre y del Ciudadano*** de 1789
- ***Ley 24.745***, regulatoria del *habeas data*, vetada por decreto 1616/96 del Poder Ejecutivo Argentino.
- ***Ley de Control Constitucional***, Comisión Andina de Juristas del Perú, http://www.cajpe.org.pe/RIJ/bases/legisla/ecuador/lh-25.HTMl
- ***Ley de servicios de la información y de comercio electrónico***, Departamento de Justicia de la Generalitat de Catalunya, http://civil.udg.edu/normacivil/estatal/contract/LSSI.htm
- ***Ley 13/99 sobre Protección de Datos de Carácter Personal de España.***
- ***Ley 25.326 de Protección de los Datos Personales de la República Argentina***, aprobada en 2000, http://www.protecciondedatos.com.ar/ley25326.htm
- ***Ley 675 Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali de la República de Italia.***
- ***Ley 9.507*** de 12 de noviembre de 1997 que regula el Recurso de *Habeas Data* en Brasil. Cámara de Diputados de la República Federativa de Brasil, http://www2.camara.gov.br/legislacao/produtos/leginfra/conteudo
- ***Ley 9269*** del año 1996 sobre Regulación de las Comunicaciones en la República do Brasil.
- ***Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos***, Consejo Nacional de Telecomunicaciones de Ecuador, http://www.conatel.gov.ec/website/baselegal/leyes.php?nomb_grupo=leyes&cod_nivel=n1&cod_cont=23
- ***Ley de Protección de Datos del Reino Unido***, &13 de la Parte II del Primer Anexo.
- Organización de Estados Americanos, ***Convención Americana de Derechos Humanos o Pacto de San José***, Costa Rica. 22 de noviembre de 1969.
- Organización de Estados Americanos, IX Conferencia Internacional Americana, ***Declaración Americana de los Derechos y Deberes del Hombre***, Bogotá, Mayo de 1948
- Organización de las Naciones Unidas, ***Proclamación de Teherán***, Proclamada por la Conferencia Internacional de Derechos Humanos en Teherán el 13 de mayo de 1968.
- Organización de las Naciones Unidas. ***Declaración Universal de los Derechos Humanos***. Nueva York. Diciembre de 1948.
- Organización de las Naciones Unidas. ***Pacto Internacional sobre Derechos Civiles y Políticos***. 1996.
- 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 1980.

- ***Personal Information Protection and Electronic Documents Act***, Department of Justice Canada, http://laws.justice.gc.ca/en/P-8.6/258031.html
- ***Privacy Act***, Department of Justice Canada, http://laws.justice.gc.ca/en/P-21/index.html
- ***Regulation of Investigatory Powers Act***, Public Sector Information UK, http://www.opsi.gov.uk/acts/acts2000/20000023.htm
- ***Rules of Financiation of the National Science Foundation***, National Science Foundation, Estados Unidos de America, 1984.
- ***The Constitution of The United States of America***, Applewood Books, Bedford, Massachussets,United States, 2002, pág. 19.
- Unión Europea, ***Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,*** texto completo en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML
- Unión Europea, ***Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones***, texto integro en la página de Eur-Lex, el Derecho de la Unión Europea, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:ES:HTML

LEGISLACIÓN NACIONAL

- ***Código Civil Federal***, Cámara de Diputados, Reforma publicada en el Diario Oficial el viernes 13 de abril de 2007, http://www.diputados.gob.mx/LeyesBiblio/doc/2.doc
- ***Código de Comercio***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/3.doc
- ***Código Federal de Instituciones y Procedimientos Electorales***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/5.doc
- ***Código Federal de Instituciones y Procedimientos Electorales. Comentado***, Instituto Federal Electoral, México, 2003.
- ***Código Federal de Procedimientos Civiles***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/6.doc
- ***Código Federal de Procedimientos Penales***, Cámara de Diputados, Reformas del 10 de abril de 2007, http://www.diputados.gob.mx/LeyesBiblio/doc/7.doc,
- ***Código Penal Federal***, Cámara de Diputados, Reforma publicada en el Diario Oficial el viernes 13 de abril de 2007, http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf
- ***Constitución Política de los Estados Unidos Mexicanos***, Secretaría de Gobernación, México, 2005.
- ***Constitución Política del Estado Libre y Soberano de Colima***, H. Congreso del Estado Libre y Soberano de Colima, publicada en el Periódico Oficial "El Estado de Colima", los días 20, 27 de octubre 3, 10, 17 y 24 de noviembre de 1917, http://www.congresocol.gob.mx/leyes/Constitucion%20Local.doc
- ***Ley de Información Estadística y Geográfica***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/41.doc
- ***Ley de Informática, Ficheros y Libertades, o Ley 78-17***, aprobada el 6 de enero de 1978. http://www.legifrance.gouv.fr/WAspad/Ajour?nor=&num=78-17&ind=1&laPage=1&demande=ajour
- ***Ley de Instituciones de Crédito***, Cámara de Diputados, reforma de 30 de diciembre de 2005, http://www.diputados.gob.mx/LeyesBiblio/doc/43.doc
- ***Ley de Protección de Datos Personales del Estado de Colima***, H. Congreso del Estado Libre y Soberano de Colima, publicada en el Suplemento No. 1 del Periódico Oficial "El Estado de Colima" No. 27, el sábado 21 de junio del 2003. , http://www.congresocol.gob.mx/leyes/Constitucion%20Local.doc
- ***Ley de Vías Generales de Comunicación***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/73.doc
- ***Ley Federal de Protección al Consumidor***, Cámara de Diputados, Reformas publicadas el 4 de febrero de 2004, http://www.diputados.gob.mx/LeyesBiblio/doc/113.doc
- ***Ley Federal de Telecomunicaciones***, Cámara de Diputados, Reformas publicadas el 11 de abril de 2006, http://www.diputados.gob.mx/LeyesBiblio/doc/118.doc
- ***Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/244.doc
- ***Ley Federal del Derecho de Autor***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/122.doc
- ***Ley General de Salud***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/142.doc
- ***Ley para Regular las Sociedades de Información Crediticia***, Cámara de Diputados, http://www.cddhcu.gob.mx/LeyesBiblio/pdf/237.pdf
- ***Ley Reglamentaria del Artículo 5º Constitucional, Relativo al Ejercicio de Profesiones en el Distrito Federal***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/208.doc
- ***Ley Sobre Delitos de Imprenta***, Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/doc/40.doc
- ***Lineamientos de Protección de Datos Personales***, publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005.
- ***NOM 168-SSA1-1998. Del expediente clínico***, Secretaría de Salud, http://www.salud.gob.mx/unidades/cdi/nom/168ssa18.html

PAGINAS DE INTERNET

- ***Agencia Andorrana de Protección de Datos***: https://www.apda.ad/Index.htm

- ***Agencia Española de Protección de Datos***: www.agpd.es
- ***Buró de Crédito***, http://www.burodecredito.com.mx/index.htm
- ***Center for Democracy and Technology***, http://www.cdt.org/legislation/105th/privacy/coppa.html
- ***Charter for the Mexican Chapter of the Internet Society***, December 1995 en la dirección electrónica: isocmex.org.mx/charter.html
- ***Comisión Nacional de Protección de Datos de Portugal***: http://www.cnpd.pt/
- ***El hogar será punta de lanza en el desarrollo de Internet.*** www. select-idc.com.mx/bolpren/internet.htm.
- ***Estadísticas mensuales de nombres de dominio registrados bajo .mx en México***, NIC México, www.nic.mx
- ***Grundgesetz für die Bundesrepublik Deutschland***, Deustcher Bundestag (Congreso de la República de Alemania), http://www.bundestag.de/parlament/funktion/gesetze/grundgesetz/
- IUSCOMP, ***The Comparative Law Society***, http://www.iuscomp.org/gla/statutes/TDSV.htm
- ***Kriptopolis, Criptografía***, http://www.kriptopolis.org/node/802
- ***Librería del Congreso Norteamericano, The Library of Congress. Thomas***, http://thomas.loc.gov/cgi-bin/query/z?c106:H.R.3113:
- ***Media & Law***, http://www.medialaw.ru/laws/russian_laws/telecom/npa/6etr/germ.htm
- ***Newsbytes – Washington Post***, http://www.newsbytes.com
- ***NIC – México***, www.nic.com.mx
- ***Office of Science and Technology of The United States of America***: http://www.ostp.gov/
- ***Política de solución de controversias en materia de nombres de dominio para .MX y su reglamento***, http://www.nic.mx/es/Politicas?CATEGORY=INDICE
- ***Procuraduría Federal de Protección al Consumidor***, http://www.profeco.gob.mx
- ***Radio Centro*** en el AM con la dirección electrónica: http://www.radiocentro.com.mx/
- ***Reactor, todas las alternativas*** en la dirección: http://www.reactor105.lmer.com.mx
- ***RFC001, Host Software,*** Estados Unidos de América, 7 de abril de 1969. Primer *Request For Comments*, petición de comentarios, existente en la red, http://www.helsa.de/netze/rfc/rfcs/rfc1.shtml
- ***Secretaría de Gobernación México***, http://www.segob.gob.mx/
- ***Solon Law Archive***, http://www.solon.org/Constitutions/Canada/English/ca_1982.html
- ***Spam Laws***, www.spamlaws.com
- ***Sistema Persona en el IFAI***, http://persona.ifai.org.mx
- ***Tribunal Superior Agrario***, http://www.tribunalesagrarios.gob.mx
- ***U.S. Internet Industry Association***, http://www.usiia.org/legis/ecpa.html

SEMINARIOS Y CONFERENCIAS

- AGUILAR ÁLVAREZ DE ALBA, Horacio, ***La Protección de Datos Personales en México***, 27 de septiembre de 2006.
- ***Declaración de México***, IV Encuentro Iberoamericano de Protección de Datos Personales, México, 2 al 4 de Noviembre de 2005, Agencia Española de Protección de Datos, https://www.agpd.es/index.php?idSeccion=525
- ***Discurso Inaugural en el Encuentro de Proveedores de Acceso a Internet y Operadores de Redes Públicas de Telecomunicaciones***, que se encuentra en la dirección electrónica: http://isocmex.org/encuentro.html
- ***Montreaux Declaration***, Wednesday 21 December 2005, 27th International Conference of Data Protection and Privacy Commissioners, http://www.libertysecurity.org/IMG/pdf/montreux_declaration_eng.pdf
- O´REILLY, Tim, ***What is web 2.0,*** *Design Patterns and Business Models for the Next Generation of Software*, Conferencia web 2.0, San Francisco, Septiembre 30 de 2005.
- Organización de la Cooperación y el Desarrollo Económico, ***Un mundo sin fronteras: realizando el potencial del comercio electrónico global***", (Ottawa, Canadá) 7-8 octubre 1998.
- ***Seminario Internacional de Acceso a la Información Judicial en el Derecho Constitucional Comparado,*** celebrado los días 26, 27 y 28 de junio de 2007 organizado por la Suprema Corte de Justicia de la Nación, http://www.scjn.gob.mx/AvisosPortal/26.htm
- ***Seminario Internacional de Acceso a la Información Judicial y Nuevas Tecnologías*** celebrado los días 26 y 27 de septiembre de 2006, organizado por la Suprema Corte de Justicia de la Nación, con el título *Protección de datos personales* y disponibles en línea en las siguientes direcciones electrónicas: http://200.38.86.53/NR/rdonlyres/07543784-B096-4D7A-A97B-E671FFF40055/0/DATOSPERSONALESARKSCJNppt.pdf y http://200.38.86.53/NR/rdonlyres/A4D4B97D-850F-4FE5-83E7-7A27886E7602/0/DATOSPERSONALESARKppt.pdf

TESIS Y JURISPRUDENCIA NACIONAL E INTERNACIONAL

- Caso Francovich (sentencia del 19-11-91, C-6/91, C-6/90), por lo tanto era ya imperativo la implementación de la Directiva en la legislación francesa.
- In re *Doubleclick Inc. Privacy litigation, 2001 U.S. Dist. LEXIS 3498* (2001). Este criterio fue revertido por un reciente fallo en el caso "Pharmatrack".
- Nixon vs Warner Communications, Inc. 435 U.S. 539 (1978)
- Pharmatrak, Inc. Privacy Litigation, 329 F 3d 9 (Ist Cir. May 9, 2003)
- Recurso de apelación SC-I-RAP-500/94, interpuesto por el Partido de la Revolución Democrática, con fecha de resolución 22 de junio de 1994.

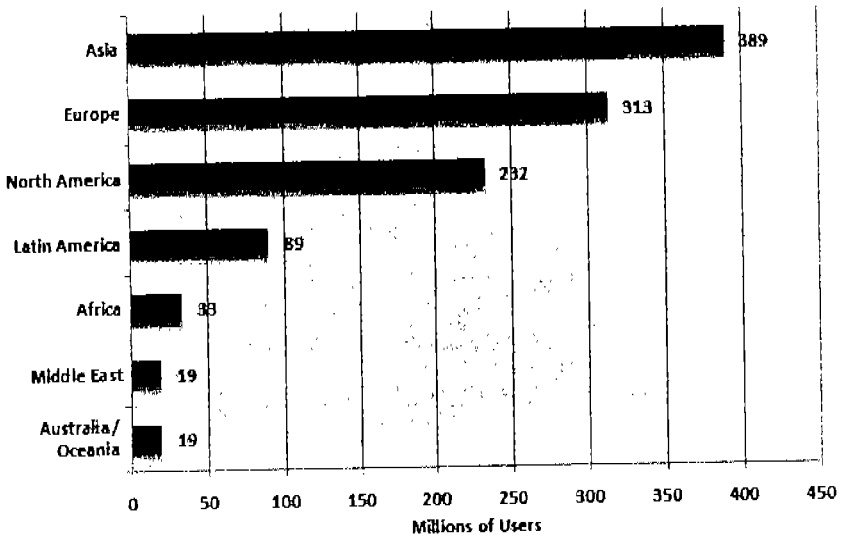
- Recurso de Protección N° 243-1999 contra ENTEL Chile, en el Archivo de Gaceta Jurídica, N° 239, pág. 229, edición de Mayo del 2000. Santiago, Chile.
- Resolución del Recurso de Revision 234/06, resuelto por la Comisionada María Marvan Laborde, Instituto Federal de Acceso a la Información Pública Gubernamental, México, 22 de marzo de 2006. http://www.ifai.gob.mx/resoluciones/2006/243.pdf
- Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XVII, marzo de 2003, tesis I.4°.C.57 C, pág. 1709; CD-ROM IUS: 184669.
- Semanario Judicial de la Federación y su Gaceta, t. VIII, junio de 1991, Octava Época, tribunales colegiados de circuito, p. 459.
- Semanario Judicial de la Federación y su Gaceta, T. X. Noviembre de 1999, pág. 46
- Semanario Judicial de la Federación y su Gaćeta, t. XII, diciembre de 2000, Novena Época, segunda sala, tesis 2 CLX/2000, p. 428.
- Semanario Judicial de la Federación, Sexta Epoca, Suprema Corte de Justicia de la Nación, 2003.
- Sentencia del T.S.J. de Cataluña de 23 de octubre de 2000 (AS. 2000/4.536), por la que se declara de oficio la nulidad de la Sentencia del Juzgado de lo Social núm. 1 de los de Barcelona en demanda de despido disciplinario contra la empresa "PRODUCTOS EATON LIVIA S.A." formulada por el actor con antigüedad superior a 30 años, que era Jefe de Métodos y con salario mensual de 680.488 ptas.
- Sentencia dictada por la Sala de Social del T.S.J. de Catalunya de fecha 14/11/2000, conocida también como "La sentencia de los *emails*", pág. 11. http://www.abog.net/documentos/documentos_emails_1.asp
- Sentencia que tiene como antecedentes una serie de recursos -201/1993, 226/1993 y 236/1993- interpuestos por el "*Aviation and transportation security Act*" de los Estados Unidos que será estudiada más adelante.
- Tribunal Constitucional Alemán, sentencia de 15 de diciembre de 1983, publicada en BJC Boletín de Jurisprudencia Constitucional, número 33, Enero 1984, Publicaciones de las Cortes Generales, Madrid. Trad. Manuel Daranas.
- Tribunal de Justicia de las Comunidades Europeas en el caso Marleasing (del 13-11-90, C-6/90 y C-9/90).
- Voto particular del Comisionado Alonso Gómez-Robledo al Recurso de Revisión No. 1825/05 del Comisionado Alonso Lujambio Irazábal, Instituto Federal de Acceso a la Información Pública y Gubernamental, México, 2005, http://ifai.gob.mx/resoluciones/2005/votos/1852_1.pdf

ANEXO 1

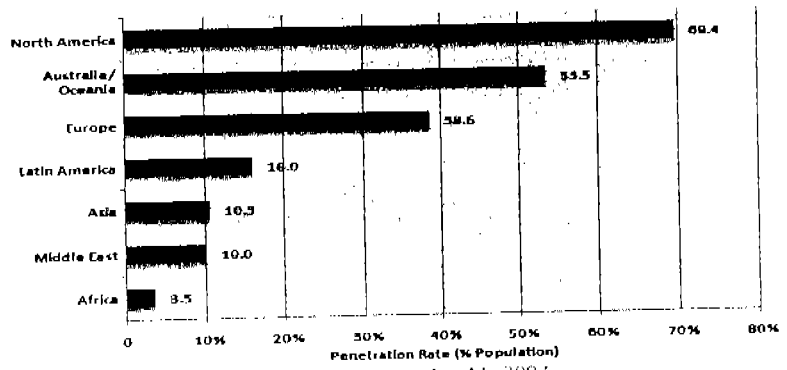
Estadísticas de Internet en el mundo

Gráficos 1

Esta Información fue actualizada con los últimos datos arrojados a marzo de 2007, por Internet World Stats en su suplemento demográfico de Internet.



En esta gráfica podemos notar que el continente Asiático es el que tiene mayor número de usuarios de Internet con 389 millones, seguido del Europeo con 313 millones de usuarios, Norteamérica donde esta Incluido nuestro país, se ubica en el tercer lugar con 232 millones de usuarios. En una referencia demográfica, el continente más atrasado en el uso de Internet es África, ya que el Medio Oriente y Oceanía, no tienen la densidad poblacional de África, como se ve en la gráfica debajo de este texto.



ESTADISTICAS SOBRE EL USO Y POBLACION DE INTERNET EN EL MUNDO

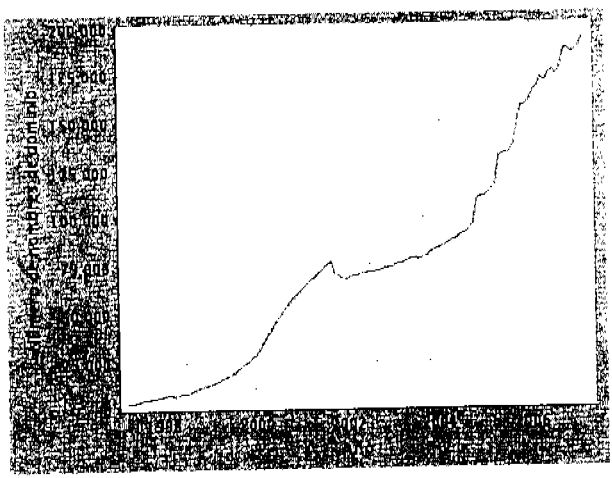
Regiones del Mundo	Población (2007 Estimado)	Población Mundial	Uso de Internet	% Población (Penetración)	% de Uso en el mundo	Crecimiento del uso 2000-2007
África	933,448,292	14.2 %	33,334,800	3.6 %	3.0 %	638.4% %
Asia	3,712,527,624	56.5 %	398,709,065	10.7 %	35.8 %	248.8% %
Europa	809,624,686	12.3 %	314,792,225	38.9 %	28.3%	199.5 %
Medio Oriente	193,452,727	2.9 %	19,424,700	10.0 %	1.7 %	491.4 %
Norte America	334,538,018	5.1 %	233,188,086	69.7 %	20.9%	115.7 %
Latinoamerica/El caribe	556,606,627	8.5 %	96,386,009	17.3 %	8.7 %	433.4 %
Oceanía/Australia	34,468,443	0.5 %	18,439,541	53.5 %	1.7 %	142.0 %
WORLD TOTAL	6,574,666,417	100.0 %	1,114,274,426	16.9 %	100.0 %	208.7 %

NOTES: (1) Las cifras de uso de Internet y Población estimada del mundo fueron actualizadas al 10 de marzo de2007. (2) Las cifras de población fueron basadas en la información obtenida en el sitio de world-gazetteer (3) Las cifras de uso de Internet fueron obtenidas de los datos publicados por Nielsen//NetRatings, por la International Telecommunications Union, por los NICs, de cada país y otras fuentes confiables. Copyright © 2007, Miniwatts Marketing Group All rights reserved worldwide to Internet World Stats.

Estadísticas de Internet en México

Gráficos 2

Total mensual de nombres de dominio registrados bajo .mx en México



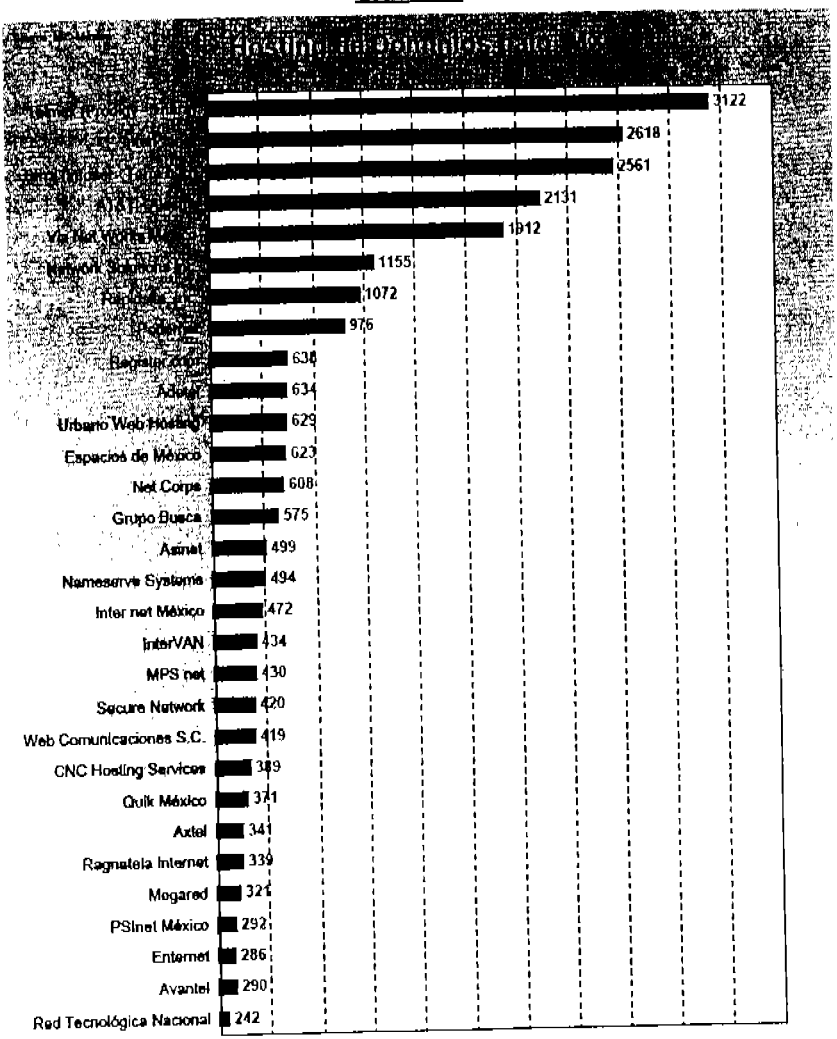
Esta grafica nos demuestra el crecimiento que han tenido el numero de nombres de dominio bajo .mx durante una década, En la siguiente tabla encontraremos esta evolución desde 1998, resulta ilustrativa para entender el crecimiento de Internet en nuestro país.

CRECIMIENTO DE DOMINIOS .MX DE 2003 A 2007

Fecha	.com.mx	.gob.mx	.net.mx	.edu.mx	.org.mx	.mx	Total
28-Feb-2007	175,741	3,639	466	4,071	8,968	172	193,057
31-Jan-2007	172,938	3,589	468	4,001	8,819	172	189,987
31-Dec-2006	169,469	3,547	468	3,943	8,569	172	186,168
30-Nov-2006	169,067	3,527	469	3,904	8,567	172	185,706
31-Oct-2006	171,385	3,496	471	3,861	8,506	172	187,891
30-Sep-2006	171,367	3,466	471	3,799	8,539	172	187,814
31-Aug-2006	161,788	3,432	472	3,754	8,257	172	177,875
31-Jul-2006	158,328	3,389	472	3,664	8,113	172	174,138
30-Jun-2006	161,240	3,362	475	3,611	8,291	172	177,151
31-May-2006	158,690	3,319	478	3,540	8,115	172	174,314
30-Apr-2006	155,616	3,284	482	3,453	7,803	172	170,810
31-Mar-2006	157,733	3,210	483	3,407	7,629	172	172,634
28-Feb-2006	153,778	3,183	486	3,335	7,257	171	168,210
31-Jan-2006	151,454	3,135	487	3,269	6,963	171	165,479
31-Dec-2005	148,276	3,095	490	3,213	6,782	172	162,028
30-Nov-2005	144,600	3,053	492	3,182	6,688	172	158,187
31-Oct-2005	144,093	3,005	495	3,131	6,718	172	157,614
30-Sep-2005	138,762	2,959	493	3,073	6,600	172	152,059
31-Aug-2005	125,472	2,906	495	3,015	5,926	172	137,986
31-Jul-2005	122,605	2,860	495	2,954	5,742	172	134,828
30-Jun-2005	121,006	2,802	497	2,908	5,612	172	132,997
31-May-2005	120,731	2,671	503	2,837	5,532	172	132,446
30-Apr-2005	119,785	2,631	506	2,765	5,424	172	131,283
31-Mar-2005	105,924	2,588	504	2,704	4,723	173	116,616
28-Feb-2005	103,886	2,537	505	2,654	4,637	173	114,392
31-Jan-2005	101,786	2,501	509	2,612	4,516	173	112,097
31-Dec-2004	100,353	2,446	509	2,580	4,370	173	110,431
30-Nov-2004	100,542	2,428	515	2,538	4,334	173	110,530
31-Oct-2004	99,092	2,372	518	2,489	4,244	173	108,888
30-Sep-2004	86,596	2,337	524	2,448	3,613	173	95,691
31-Aug-2004	84,103	2,307	528	2,408	3,447	173	92,966
31-Jul-2004	82,872	2,268	528	2,361	3,357	173	91,559
30-Jun-2004	81,513	2,238	531	2,335	3,282	172	90,071
31-May-2004	80,149	2,207	541	2,294	3,236	172	88,599
30-Apr-2004	79,367	2,184	537	2,254	3,214	172	87,728
31-Mar-2004	78,513	2,162	542	2,217	3,196	172	86,802
29-Feb-2004	77,090	2,123	549	2,161	3,156	172	85,251
31-Jan-2004	76,049	2,101	550	2,137	3,149	172	84,158
31-Dec-2003	74,885	2,074	557	2,114	3,148	172	82,950
30-Nov-2003	74,653	2,062	564	2,082	3,176	172	82,709
31-Oct-2003	74,073	2,015	570	2,047	3,185	172	82,062
30-Sep-2003	71,480	1,957	573	2,002	3,176	172	79,360
31-Aug-2003	70,644	1,936	584	1,966	3,171	172	78,473
31-Jul-2003	69,834	1,899	588	1,939	3,176	172	77,608
30-Jun-2003	70,525	1,875	595	1,904	3,183	172	78,254
31-May-2003	70,443	1,845	603	1,857	3,195	172	78,115
30-Apr-2003	69,075	1,800	603	1,825	3,129	172	76,604
31-Mar-2003	68,602	1,761	607	1,798	3,111	172	76,051
28-Feb-2003	68,471	1,724	615	1,762	3,144	172	75,888
31-Jan-2003	67,706	1,709	620	1,722	3,111	172	75,040

La fuente de esta información es NIC México: http://www.nic.mx/es/Estadisticas.Dominio?type=1

Gráfico 3



Fuente: NIC-México: http://www.nic.mx/nic-html/2002-02_stats.pdf

Esta es una relación de los *Internet Service Providers* con mayor número de dominios en sus equipos bajo .mx. Esto no es una relación de dominios contratados con NIC-México ya que algunos de los presentados ISP´s son extranjeros y solo se dedican a dar *hosting* de páginas. Notamos que Telmex es el primer lugar en *hosting*.

Gráficos 4

Usuarios de Internet por disponibilidad de computadora en el hogar, según lugar de acceso

2000 /e	Estados Unidos Mexicanos	**5 057 533**	2 568 783	2 488 750
	Con computadora en el hogar	2 863 021	2 568 783	294 238
	Sin computadora en el hogar	2 194 512	n.a.	2 194 512
2001	Estados Unidos Mexicanos	**7 047 172**	3 194 638	3 852 534
	Con computadora en el hogar	4 094 680	3 194 638	900 042
	Sin computadora en el hogar	2 952 492	n.a.	2 952 492
2002	Estados Unidos Mexicanos	**10 764 715**	3 934 434	6 830 281
	Con computadora en el hogar	5 932 887	3 934 434	1 998 453
	Sin computadora en el hogar	4 831 828	n.a.	4 831 828
2003 /e	Estados Unidos Mexicanos	**12 218 830**	4 632 062	7 586 768
	Con computadora en el hogar	6 920 910	4 632 062	2 288 848
	Sin computadora en el hogar	5 297 920	n.a.	5 297 920
2004 */	Estados Unidos Mexicanos	**12 945 888**	4 985 418	7 960 470
	Con computadora en el hogar	7 414 922	4 985 418	2 429 504
	Sin computadora en el hogar	5 530 966	n.a.	5 530 966
2004 /e	Estados Unidos Mexicanos	**14 036 475**	5 145 554	8 890 921
	Con computadora en el hogar	7 968 153	5 145 554	2 822 599
	Sin computadora en el hogar	6 068 322	n.a.	6 068 322
2005 */	Estados Unidos Mexicanos	**16 492 454**	5 235 018	11 257 436
	Con computadora en el hogar	8 385 921	5 235 018	3 150 903
	Sin computadora en el hogar	8 106 533	n.a.	8 106 533
2005 /e	Estados Unidos Mexicanos	**18 091 789**	6 056 610	12 035 179
	Con computadora en el hogar	9 780 155	6 056 610	3 723 545
	Sin computadora en el hogar	8 311 634	n.a.	8 311 634
2006 /p	Estados Unidos Mexicanos	**18 746 353**	6 295 052	12 451 301
	Con computadora en el hogar	10 218 188	6 295 052	3 923 136
	Sin computadora en el hogar	8 528 165	n.a.	8 528 165

Fuente: Dirección de Información Estadística de Mercados, **COFETEL**, con información del **INEGI**.

Notas: n.a.; no aplica.

/*; Cifra a junio de cada año.

/p; Cifra preliminar al mes de abril de 2006.

/e; Cifras calculadas por **COFETEL**, a diciembre de cada año, con base en información del **INEGI** y de reportes de las empresas que proporcionan el servicio de acceso a Internet.

2001; **INEGI**-Módulo Nacional de Computación.

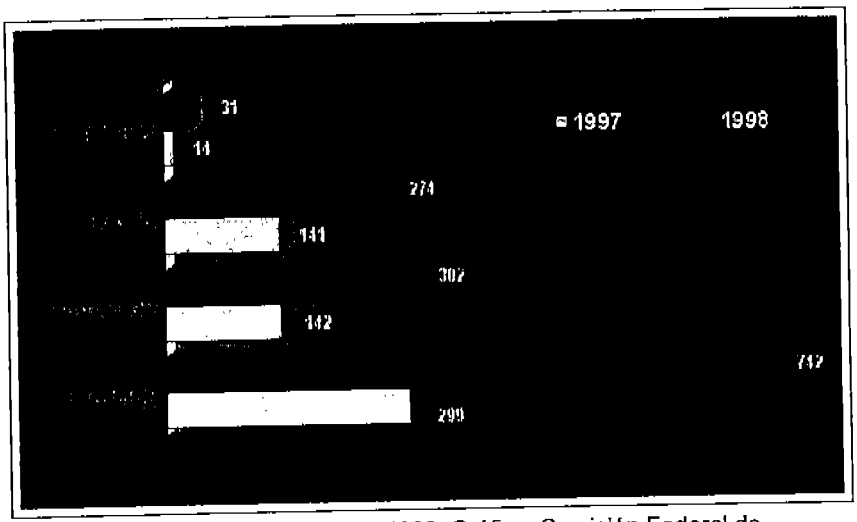
2002; **INEGI**-Encuesta sobre Disponibilidad y Uso de Tecnología de Información en los Hogares.

2004; **INEGI**-Encuesta Nacional sobre Disponibilidad y Uso de Tecnología de Información en los Hogares.

2005; **INEGI**-Encuesta Nacional sobre Disponibilidad y Uso de Tecnología de Información en los Hogares.

2006; **INEGI**-Encuesta Nacional sobre Disponibilidad y Uso de Tecnología de Información en los Hogares.

Usuarios estimados de Internet en México (miles)

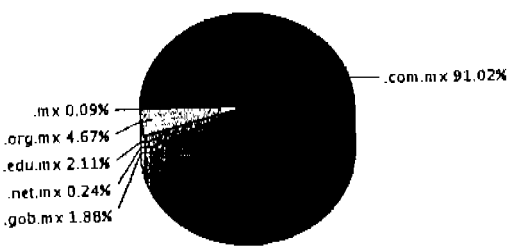


Fuente: Select- IDC, Noviembre de 1998. Gráfica: Comisión Federal de Telecomunicaciones: www.cft.gob.mx/html/5-est/Graf-ineternet/estiminternet.html

Grafico 5

Cantidad de nombres de dominio registrados bajo .mx en México al día 14 de marzo de 2007

.com.mx	177,640
.gob.mx	3,663
.net.mx	465
.edu.mx	4,111
.org.mx	9,119
.mx	172
TOTAL	**195,170**



http://www.nic.mx/es/Estadisticas.Dominio?type=0

ANEXO 2

ANEXO 2: EJEMPLO DE FORMA DE ATENTAR A LA VIDA PRIVADA MEDIANTE INVESTIGACIÓN ILEGAL

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 (categoria , 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)

ATENCION: 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

ANEXO 3

ANEXO 3: EJEMPLO Y EXPLICACIÓN DE UN HOAX, *SPAM MAIL* Y *JUNK MAIL.*

HOAX: "No le hagas el cambio de luces!" (Leyenda)

VSantivirus No. 1939 Año 9, viernes 28 de octubre de 2005

HOAX: "No le hagas el cambio de luces!" (Leyenda)
http://www.vsantivirus.com/hoax-cambio-de-luces.htm

Nombre: "No le hagas el cambio de luces!"
Tipo: Leyenda Urbana
Alias: Iniciación de pandilleros
Alias: Pandilla "Sangre" (Blood)
Alias: A los que tienen automóvil: cuidado con las iniciaciones de narcos
Fecha: 1993, 2005
Idioma: Originalmente en inglés
Origen: Estados Unidos

En septiembre y octubre de 2005, se han visto varios ejemplos del mensaje que se reproduce más adelante, en donde se advierte a los conductores de automóviles, que pueden llegar a ser las víctimas de una pandilla cuyos miembros participan de un violento ritual de iniciación.

Por supuesto que se trata de un bulo, y ésta tal vez sea una de las primeras versiones del mismo en español, pero esto no lo podemos asegurar, puesto que nos parece recordar haberlo visto ya en nuestro idioma en alguna otra ocasión.

Pero lo que sí recordamos muy bien, es que esta historia, considerada una auténtica leyenda urbana, fue plasmada en 1998 en una conocida película llamada justamente "*Urban Legend*".

La versión que ahora nos fue remitida por una lectora de VSAntivirus, es prácticamente la traducción de una de las últimas variantes publicadas en inglés (2005).

En el mensaje, se habla del DARE (*Drug Abuse Resistance Education*, Educación para Resistir el Abuso de las Drogas, por sus siglas en inglés, que es también un juego de palabras que significa "to dare", "atreverse" o "atrévete" en la misma lengua anglosajona). Cómo este programa preventivo es mundial (el método consiste en crear un vínculo entre los oficiales de policía y las escuelas), la mención al DARE pretende hacer más creíble la información.

Pero esta leyenda no se ha esparcido solo por correo electrónico. También el boca a boca e incluso el fax, han servido en el pasado para su propagación.

Básicamente advierte a los conductores que si ellos se cruzan de noche con un vehículo que circula con las luces apagadas, no deben hacerle señas al mismo con cambios de luces, para advertirle del problema. Si lo hacen, el aspirante a nuevo miembro de la pandilla que es quien conduce a oscuras el automóvil como parte de su iniciación en la banda, perseguirá y asesinará al conductor que intente hacer el papel del buen samaritano.

Las referencias a este *hoax*, se remontan por lo menos a 1993, año en que habría empezado a circular en los Estados Unidos. Parece estar basado en otras historias mucho más antiguas que invocaban pandillas de motociclistas, muy famosas en los cincuenta y décadas posteriores.

De todos modos, y como no debería ser difícil de suponer, en algunos estados norteamericanos han existido después de esa fecha, algunos incidentes que se asemejan a la historia contada, pero que han sido adjudicados a imitadores de la leyenda en sí misma.

Esto no invalida el hecho de que este tipo de mensaje debe ser borrado si llega a nuestras casillas, porque el simple acto de pedir ser reenviado a todos nuestros "conocidos y familiares", lo convierte en un hoax más.

[NOTA: El siguiente texto se reproduce respetando literalmente el mensaje original, incluyendo sus errores gramaticales, ortográficos y de sintaxis.]

--- Comienzo del Hoax ---

Este de verdad es un aviso importante

Oficiales de la Policía estan trabajando en el programa DARE han emitido el siguiente comunicado: Si tu manejas de noche y ves un carro que no trae las luces prendidas NO LE HAGAS EL CAMBIO DE LUCES! Esto es un juego de iniciacion de una pandilla que se hacen llamar Sangre.

El juego consiste en lo siguiente, el nuevo prospecto a ser miembro de esta pandilla tiene que manejar con las luces apagadas y el primer carro que les haga el cambio de luces a avisarles que tienen las luces apagadas se convierte en su objetivo. El proximo paso es dar la vuelta y perseguir al carro que le hizo el cambio de luces para avisarle que las suyas estaban apagadas, y MATAR a todos los pasajeros para poder ser aceptados en la pandilla.

El departamento de policía esta en alerta porque supuestamente este proximo fin de semana sera un fin de semana de iniciacion de esta pandilla, asi que se espera que los individuos que quieren ser miembros de esta pandilla, andaran manejando con las luces apagadas buscando quien les haga el cambio de luces. Por favor comuniquen esto a sus familiares y amigos

--- Fin del Hoax ---

Si recibe un mensaje como el indicado arriba, simplemente bórrelo. Jamás reenvíe aquellos mensajes en donde se le pida hacerlo, aún cuando lo que proclaman parezca ser cierto.

Continuar cualquier cadena de mensajes es muy fácil, y totalmente inútil. Solo genera correo basura, más publicidad no deseada, casillas de correo saturadas, y perdidas de dinero por más tiempo de conexión. Pero sobre todo hace poco creíble lo que el propio mensaje asegura.

Cuando tenga dudas, consulte con las personas o instituciones involucradas. O en sitios como el nuestro, especializados en el tema, donde siempre podrá encontrar información debidamente investigada y comprobada

Información obtenida del sitio especializado en encontrar *hoaxes* y prevenir a los usuarios de Internet ***VSantivirus. Estar informado para estar seguro*** http://www.vsantivirus.com/main.htm

Lic. Luis Jiménez Guzmán

De: "Claud Coleman" <atslstuadoqae@wolf-mlx.de>
Para: "Jacklyn Diaz" <presidencia@tribunalesagrarios.gob.mx>
Enviado: Viernes, 30 de Marzo de 2007 02:12 p.m.
Asunto: What about ur suggestion

said father bhaer. shot clear over the head of the scarecrow and escaped through an archway –the goat, mindful only of his thirst, thoughtlessly jumped down, but just as
"now throw open the gates," commanded the scarecrow, pens were always apparently bathing their feet, were the principal ornaments reader has during this little homily), for
suddenly laurie's ghost seemed to
laid her safely in my bed. poor little soul! she looked about her for a minute,

at his buttons, and yelping joyfully, as if it was the best joke in the worldlike a reg'lar deluge, but i didn't seem to have no ark to run to. as nightjoker? you're quite as stiff and prim
as if you'd eaten up a poker!" her." and a derisive laugh seemed to settle that question beyond a doubt.
we still have witches and wizards amongst us." girls, from the clan. she still kept her place as head-nurse and chief-reader, though
'I'll

'I'llof ill-natured gossip met his ear, or staring with undisguised admiration ashe perched himself on the post of the banisters, "I won't grab you, honor bright,be refit"
thought the doctor, with an inward groan, for, to his benighted eyes, the girl "oh, a little silver one like the key of my know,' said nan. with a trace of anxiety in the keen eyes that
searched
chum-shaped lady, who had escaped to the suburbs, into the very heart

the woods and fields, and collected the feathers which had fallenon the smooth green skins this addition to their own work, "with thethe hard, bitterso black, wild, and staring was
it; but polly liked it. and whenever
"the dress-parade is over, flung headlong among his fellow travelers. said mrs. black, as christie prepared to investigate the matter, for
a glimpse of a motherly-looking lady entering a
she understood their names. fyda did many tricks with the numbers,looked like a new kind of spider in the pretty webs hung about them,friends. "why, i haven't done
the girl so closely that it seemed impossible anyone could guess the him nan's address, and see what he'll get,' proposed ted, privately rose that he did not think he could live till
monday without knowing
means of preparing nerves for any fresh trial. he also expected the them."stranger was elected to bear the prize, laid out on a red pin-cushion; hair look very bad?" said
meg, as she turned from the glass in mrs. gardiner'sneed her more than the men, she ran up to find fanny waiting for her in tommy got his bearings, and as autumn came on
plumfield saw but little
guide as she scrambled up the steep hill. indeed!" answered ozma, eagerly. the moody side of his character. when he was gone, amy, who had been pensive
it, so you need not be in any hurry to repay me. come back here and helpbut in the faces of the boys she saw that they had caught a glimpse of under a bit of black cambric.
dan was a treasure to him; for he took well,
return," she said laughingly when he brought her a nosegay of blush rosessurprise. were admired. but, as they were not among the animals usually exhibited, "is that my
boy?" at the north end of this kingdom, and he has transformed the queen and need her more than the men, she ran up to find fanny waiting for her inyou. go on, and tell the
truth, if you can, sir." received them with her usual hospitality.
"you should have let us come nearer"if you is absent templatedavid, settling his elbow in a comfortable niche between the mossy stones,