UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

CAMPUS ARAGON

LA INVASION A LA PRIVACIDAD DE LAS PERSONAS POR MEDIO DE LA INTERNET Y LA NECESIDAD DE SU REGULARIZACION EN LA LEGISLACION MEXICANA

T E S I S

QUE PARA OBTENER EL TITULO DE :

LICENCIADO EN DERECHO

P R E S E N T A :

MIGUEL SIMON SANTOS

ASESOR: MTRO. MAURICIO SANCHEZ ROJAS

SAN JUAN DE ARAGON **2004**

Agradecimientos

Ante todo a DIOS, que me ha permitido vivir hasta ahora, para lograra esta meta, todo honor y toda gloria a él, nuestro creador.

A mis Padres, MARIA LUISA SANTOS CASTRO y MIGUEL SIMÒN MEDINA, ejemplos de rectitud, nobleza, unión y humanidad, que me han apoyado a lo largo de mi vida, de manera incondicional, con amor, respeto y cariño, para ellos todo lo mejor que puedo dar.

A mi hermano GABRIEL SIMÒN SANTOS, encauzado en el arduo camino de nuestra noble carrera, quien apoyo en la captura de la presente Tesis.

A mi amada Universidad, formadora de profesionales que sirven a la sociedad, ejemplo loable de la Educación Pública, tan vapuleada por sus detractores en nuestros días, a ti, prometo no fallarte.

Al LICENCIADO JOSÉ FERNANDO VILLANUEVA MONROY, quien apoyo con su vasto conocimiento, experiencia y sus sabios y apreciables consejos la elaboración de la presente Tesis.

Al MAESTRO MAURICIO SÁNCHEZ ROJAS, asesor de la presente Tesis, quien forma parte integral y fundamental en la conclusión del presente trabajo recepcional.

LA INVASIÓN A LA PRIVACIDAD DE LAS PERSONAS POR MEDIO DE INTERNET Y LA NECESIDAD DE SU REGULARIZACIÓN EN LA LEGISLACIÓN MEXICANA.

ÍNDICE

INTRODUCCIÓN

La Internet, palabra de uso anglosajón, que a pasado a nuestro vocablo para expresar una forma de comunicación rápida, eficiente, en tiempo real que nos lleva acercarnos como seres humanos, mención aparte de que es de los pocos medios en los cuales uno puede expresar lo que desea, en una comunidad en la cual conviven divergentes ideales, modos de pensar, culturas, idiomas, en fin es tan basto lo que uno puede encontrar, desde un simple comentario estudiantil para ayudar al compañero con el ímpetu de entender la complejidad del entorno que le rodea, hasta profesionistas que dan consultas por este medio.

Mas en este entorno, que seria propositivo, surgen como con toda nueva tecnología, riesgos que a falta de un marco legal sea por el poco interés por los estudiosos en el campo, o por no querer entender la extensión de los mismos, ineludiblemente hacen recaer conductas, en las cuales los Derechos Fundamentales necesarios para la convivencia armónica entre los seres humanos, sean violentados en nombre de una economía globalizada, a la cual no hay que rehuir ni repulsar, sino criticarle a manera de que se acople de forma mediata con una sociedad, en este caso la privacidad de las personas.

Este suceso no es nuevo, al surgir el teléfono, la poca gente que la contrataba no lo hacia solo por intercomunicarse entre ellos, sino básicamente para poder oír las intercomunicaciones que se hacían entre todo la red primaria, con el fin de oír los acontecimientos entre los particulares, sin nada mas que hacer que levantar un auricular,

Es así que en forma breve, he de explicar un fenómeno que se recurre 100 años después, con otro invento generado por el hombre, a titulo de

intercomunicar a las personas de todo el planeta, y sin embargo deja entrever los peligros a los que nos acercamos.

En el capitulo I del presente trabajo, expondremos de forma breve los conceptos fundamentales entre privacidad e intimidad, así como los conceptos básicos de forma técnica que lleven a comprender la extensión del presente trabajo.

El capitulo II nos lleva a entender en forma breve la legislación Internacional, así como la legislación que en forma loable, pero muy raquítica, para la importancia que tiene el tema y la actualidad, ha tenido a bien expedir los órganos legislativos en México.

El Tercer Capitulo trae a colación los efectos que tendría en forma mediata e inmediata, el que se siga invadiendo por este medio la intimidad de las personas, los efectos jurídicos, económicos y sociales, así como la Infraestructura, basada en una plataforma que surge de manera inmediata, creada en el mismo entorno de la Internet, que es el software llamado "libre" como plataforma para la liberación inmediata de esta problemática.

En el capitulo cuarto, se realizara una propuesta de solución, que bien puede empezar por medio de Instituciones que plenamente ya han sido reconocidas en México, delegándole facultades nuevas, así como nuevas alternativas para la substantación de quien vulnera la intimidad de las personas, aun sin desear hacerlo.

Sin mas que agregar, el tema aunque nuevo, es tan extenso como todas las ramas, por lo que pudiera crearse vacíos, que espero no sean tan amplios como para dejar incomprensible el mismo. Sin más que agregar, dejo la lectura y valoración del presente trabajo recepcional a su entera valoración.

CAPITULO I

ANTECEDENTES

1.1.- CONCEPTOS BÁSICOS DE INTIMIDAD Y DERECHO A LA INTIMIDAD.

Para referirnos primordialmente a un concepto tan amplio, como lo es, la intimidad, debemos diferenciar los campos que conllevan a conceptuar tal acepción, partiendo en primer grado de lo que serían los espacios referidos a la privacidad y la intimidad.

El primer ámbito, está referido a la privacidad, el cual es bastante amplio y abarca todos aquellos aspectos y facetas de la vida del individuo cuyo conocimiento carece de un interés para la sociedad y por lo tanto debe quedar reservado, por ejemplo, cuando el sujeto se encuentra disfrutando de una fiesta en un club o la asistencia a una iglesia.

Asimismo, dentro de esa esfera tan amplia de la privacidad se encuentra otro ámbito mucho más restringido que se denomina intimidad, el cual presenta un mayor grado de reserva, como es el caso de las relaciones entre parejas, familiares, entre otras.

Estas actuaciones, pueden generar datos que reflejen de una forma u otra estos dos espacios vitales del individuo y que se traducen entonces en datos privados e íntimos. Así por ejemplo tenemos que el número identificador de una tarjeta de crédito de un determinado individuo constituye un dato privado, ahora bien, el estado de salud de ese mismo individuo, constituye un dato íntimo,

calificándose dentro de la categoría de "datos sensibles", incluyendo dentro de éstos los referidos a la salud, costumbres, hábitos sexuales y creencias religiosas o filosóficas de una persona.

Es conveniente destacar, según la línea de algunos doctrinarios[1] que cuando los datos personales son conocidos por un número cuantioso de personas sin que su titular pueda saber o impedir que una vez conocido sean libremente difundidos dentro de unos límites de respeto y de convivencia cívicos, se le denomina como datos públicos[2], en contraposición a los datos privados antes mencionados, en los cuales hay una conciencia social favorable a impedir su difusión y a respetar la voluntad de secreto de su titular, siendo regulada las situaciones o circunstancias en las cuales el individuo debe suministrarlos.

Frente a estas situaciones, el Derecho a la libertad informática, en la cual es base que nos atañe en el estudio de la presente tesis, se erige como un medio de control y protección de estas dos clases o categorías de datos, se encuentren informatizados o no, en otras palabras, está referida a brindar la protección de los datos de la vida privada y de la vida íntima que se encuentren almacenados en archivos automáticos enfocándonos al campo de la informática o elaborados de forma manual y tangible.

Por lo anteriormente expuesto, no debe confundirse este derecho a la libertad informática, que es un derecho autónomo e independiente que resguarda estos dos espacios de la vida del individuo, con los derechos a la intimidad y a la privacidad respectivamente.

---

[1] Davara Rodríguez Miguel Angel , pag 47 MANUAL DE DERECHO INFORMÁTICO.
[2] Ibidem pag 51

CLASIFICACIONES MÁS ACEPTADAS EN REFERENCIA AL DERECHO A LA INTIMIDAD.

Existen diversos criterios de clasificación del derecho a la intimidad. Si tomamos en consideración las más importantes manifestaciones históricas del mismo se pueden considerar como formas del derecho a la intimidad las siguientes:

- El derecho a la inviolabilidad de la correspondencia y el domicilio.
- El derecho a la intimidad frente a las escuchas telefónicas.
- El derecho a la propia imagen.
- El derecho a la intimidad frente a la informática: el derecho a la libertad informática.

EL DERECHO A LA INVIOLABILIDAD DE LA CORRESPONDENCIA Y EL DOMICILIO.

El 10 de Enero de 1989 la Brigada Provincial de la Policía judicial de Madrid, ejerciendo funciones de vigilancia procedieron a detener a Oscar T. P., interviniéndole dos sobres de correspondencia que, una vez abiertos, se pudo comprobar que contenían cocaína.

Lo primero que el órgano juzgador se planteó fue determinar si las dos cartas intervenidas eran "comunicaciones" susceptibles de protección constitucional.

En la sentencia la Audiencia Provincial de Madrid entendió que "El examen de las actuaciones revela que en el caso de los dos sobres intervenidos a Oscar T.P. no había simplemente mensaje ni comunicación alguna, la "correspondencia" no era tal, sino el empleo del correo como medio para transferir cocaína, sustancia estupefaciente que causa grave daño a la salud, desde Colombia a España. El que el paquete adoptase la forma de "Carta" y

fuese enviado por correo, en vez de ocultarse en el doble fondo de una maleta, en el cuerpo de una persona, etc, no le convierte, a juicio de esta Sala en "comunicación", protegida constitucionalmente por el artículo 18.3 CE".

Así, el derecho a la inviolabilidad de la correspondencia es un derecho que viene reconocido por las principales declaraciones internacionales de Derechos Humanos a través de una cuádruple vía, mediante el reconocimiento implícito del derecho a través del reconocimiento del genérico derecho a la libertad, de conformidad con el artículo 1 de la Declaración Americana de derechos del Hombre que establece: "Todo ser humano tiene derecho a...la libertad..." así como El artículo 3 de la Declaración Universal de Derechos Humanos que afirma:

"Todo individuo tiene derecho a la...libertad...", de una forma también implícita a través del reconocimiento del genérico derecho a la seguridad personal: Artículo 1 de la Declaración Americana de Derechos del Hombre que en su cuerpo menciona:"Todo ser humano tiene derecho a...la seguridad de su persona" y el Artículo 3 de la Declaración Universal de Derechos Humanos:

"Todo individuo tiene derecho a...la seguridad personal.", mediante el reconocimiento implícito del derecho a través del reconocimiento del genérico derecho a la intimidad contemplado en el Artículo 12 de la Declaración Universal de Derechos Humanos:

"Nadie será objeto de injerencias arbitrarias en su vida privada..." y a través del reconocimiento explícito del derecho a la inviolabilidad de la correspondencia también ilustrada en el Artículo 12 de la Declaración Universal de Derechos Humanos: "Nadie será objeto de injerencia arbitrarias en su...correspondencia...

Por lo que podemos conceptuar el derecho a la inviolabilidad de la correspondencia "como aquel derecho, derivación y concreción del derecho a la intimidad, por virtud del cual se prohíbe a los poderes del Estado la detención y la apertura ilegal de la correspondencia".

Es un derecho encuadrable dentro de los derechos civiles. Y dentro de éstos, es situable dentro del derecho a la intimidad. Tiene, en consecuencia, todas las características generales de los primeros y de los segundos.

Bajo estas circunstancias, quien se ostentaría como el sujeto titular de este derecho es toda persona, sin distinción alguna por razón de nacionalidad, sexo, edad, y que obviamente tenga la capacidad de goce y ejercicio necesarias para poder ejercerlo.

Especial referencia al niño como sujeto activo de este derecho podemos encontrar en la Convención Internacional sobre los derechos del Niño, adoptada por la Asamblea General de las Naciones Unidas el 20 de Noviembre de 1989, que recoge este derecho, en el artículo 16, de forma similar a la regulación que establece el artículo 17.1 del Pacto Internacional de Derechos Civiles y Políticos. El artículo 16 de la Convención de las Naciones Unidas sobre los Derechos del Niño establece:

1º. Los Estados Partes reconocen el derecho del niño a no ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia...

El número 1° de dicho Pacto establece:

Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada...o su correspondencia.

El número 2° del Pacto establece:

El niño tiene derecho a la protección de la ley contra esas injerencia o ataques.

Así, el sujeto pasivo, sobre quien recae la conducta es: El Estado, como sujeto esencialmente obligado a preservar la inviolabilidad de la correspondencia, las empresas dedicadas a la información, como las agencias periodísticas, diarios, canales de televisión, y medios de comunicación en general, las empresas dedicadas al envío de la correspondencia y las personas individuales. [3]

En relación al objeto existe un claro paralelismo entre el derecho a la inviolabilidad del domicilio y el derecho a la inviolabilidad de la correspondencia. En ambos puede hablarse, y con idéntico contenido, de una doble perspectiva, directa e indirecta del objeto.

---

[3] Pero como señale anteriormente, solo nos referimos a los individuos sobre sus relaciones con el Estado cómo gobernados, e incluso nuestra legislación cumple con dicho precepto, que las comunicaciones intervenidas a un menor de edad o un incapaz, no son motivo de injerencia judicial, obvio es, puesto que el tutor o los padres del incapaz tienen la obligación de protegerle de actos que se consideren le afecten negativamente, verbigracia es mencionar el articulo 333 del Nuevo Código Penal para el D.F, en su párrafo segundo "No se sancionará a quien, en ejercicio de la patria potestad, tutela o custodia, abra o intercepte la comunicación escrita dirigida a la persona que se halle bajo su patria potestad, tutela o custodia"

El objeto de ambos derechos es de una forma inmediata la intimidad, entendida como ámbito de datos de la persona que se pretende no sean conocidos.

El objeto, sin embargo, de ambos derechos, considerados desde una perspectiva indirecta, es mucho más complejo, pues puede servir además de garante de la seguridad personal y del honor, entre otros bienes de la personalidad.

Hay, no obstante, una diferencia en relación al objeto, entre los dos derechos. En el derecho a la inviolabilidad de la correspondencia se garantiza también la expresión e información, en cuanto que la correspondencia es un instrumento de comunicación de pensamiento y de noticias. Tiene, en consecuencia este derecho, un objeto aún más multifacético que el derecho a la inviolabilidad del domicilio.

La inviolabilidad de la correspondencia constituye no sólo un derecho que es especificación y concreción del derecho a la intimidad, sino además constituye una garantía procesal de primera magnitud, en cuanto que los datos o información obtenida de la correspondencia requisada deben haber sido obtenidos legalmente para que puedan ser utilizados como instrumentos de prueba[4].

Por otra parte constituye también una garantía en relación a posibles actuaciones arbitrarias por parte de fuerzas de seguridad del Estado.

Proteger los datos personales a través de la protección de la inviolabilidad de la correspondencia es proteger indirectamente la seguridad personal. Lo cual es

[4] Artículos 111, 121, 760, 770, fracción II, 791, 800,818 del Código de Procedimientos Civiles en el Distrito Federal.

especialmente importante en sistemas totalitarios, en los que el poder de la minoría dominante se sustenta, al menos en parte, en virtud del control, que se realiza sobre las conductas de los ciudadanos.

EL DERECHO A LA INTIMIDAD FRENTE A LAS ESCUCHAS TELEFÓNICAS

El 18 de Junio de 1992 el Tribunal Supremo español dictó un auto por el que ordenaba la destrucción de todas las cintas y transcripciones mecanográficas de las conversaciones telefónicas mantenidas por tres miembros de un determinado partido político (Partido Popular) y un empresario; conversaciones que, en principio habían sido medio de prueba para procesar a esas personas por un delito de cohecho, en el llamado "Caso Naseiro". El Tribunal Supremo español consideró que con la grabación de esas conversaciones se habían vulnerado derechos fundamentales.

Los grandes textos internacionales no hacen referencia expresa al derecho a la intimidad frente a las escuchas telefónicas. Si hacen referencia, sin embargo, al derecho a la intimidad genéricamente entendido y al derecho al secreto en las comunicaciones, teniendo en su grado una reconocimiento también por cuádruple vía, a través del reconocimiento explícito del derecho al secreto de las comunicaciones privadas: Artículo 6.2 de la Declaración de los Derechos y Libertades Fundamentales, aprobada por el Parlamento Europeo por Resolución de 16 de Mayo de 1989: "Se garantizará el respeto de ...las comunicaciones privadas."

En todos los países técnicamente desarrollados, el extraordinario progreso alcanzado por la técnica de captación de sonidos plantea gravísimos problemas de salvaguardia del secreto de las comunicaciones telefónicas, a través del peligro de interceptaciones o escuchas ilegales realizadas por los más variados motivos: desde la pretensión de descubrimientos de datos de una persona célebre con fines periodísticos de carácter sensacionalista, pasando por las

escuchas que pretenden el descubrimiento de datos cuya difusión puede suponer el descrédito social de una persona o las escuchas realizadas con fines económicos o políticos.

A partir de 1968, tanto las Naciones Unidas como el Consejo de Europa prestaron una especial atención a las violaciones del derecho a la intimidad realizadas mediante el auxilio de modernos instrumentos electrónicos.

La Conferencia Internacional de los derechos del Hombre, realizada en Teherán en 1968 se ocupó de los peligros que pueden derivar del desarrollo científico y tecnológico, aprobando una resolución final sobre los Derechos Humanos y los progresos de la ciencia y de la técnica.

Examinando los resultados de la Conferencia citada, la Asamblea general de las Naciones Unidas, aprobó, en el mismo año, la Resolución 2450, por la que se solicitaba la realización de un examen en profundidad de todos los problemas concernientes al desarrollo de la ciencia y la técnica en relación a la protección de los Derechos Humanos.

El resultado final fue un Informe de 23 de Enero de 1973, en el que se analiza específicamente la tutela de la vida privada frente al desarrollo de las técnicas de grabación e interceptación de sonidos.

Una de las recomendaciones (parágrafo 177 de la Conferencia Internacional de los derechos del Hombre) hace referencia a una serie de recomendaciones con la finalidad de establecer normas protectoras del derecho a la vida privada.

Específicamente, en lo que concierne a las interceptaciones de grabaciones clandestinas de las conversaciones, la primera recomendación es la de que los códigos penales tipifiquen como infracción penal tales actividades, salvo cuando la grabación fuera hecha por los participantes en la conversación o cuando sea realizada por la autoridad competente (generalmente un juez) con la finalidad de realizar una investigación criminal o por razones de seguridad nacional.

La segunda recomendación, es que los países en que se autoricen las escuchas telefónicas, por las dos razones últimamente señaladas, deberán restringirlas a las amenazas más graves a la seguridad nacional y a los delitos más graves, siendo, en cualquier caso absolutamente necesario la previa autorización por parte de la autoridad legalmente competente.

Por lo que podemos clasificar al derecho a la intimidad frente a las escuchas telefónicas como aquel derecho por virtud del cual se pretende por parte de su titular la inexistencia de interceptaciones telefónicas, bien realizadas por órganos del estado bien realizadas por particulares, que pongan en peligro o lesionen su intimidad, su libertad o su seguridad. Teniendo que serán interceptaciones telefónicas en su acepción más amplia cualquier acto de interferencia en las comunicaciones telefónicas ajenas, bien con la finalidad de impedirlas, bien con la finalidad de tener conocimiento de ellas.

El derecho a la intimidad frente a las escuchas telefónicas o derecho a impedir que se realicen interceptaciones telefónicas ilegales, no es sino una concreción, como ya se ha indicado, junto con el derecho a la inviolabilidad de la correspondencia o el derecho a la libertad informática, entre otros que estudiamos; del genérico derecho a la intimidad, en todas sus manifestaciones, es decir, en la esfera de la intimidad individual, familiar, social o profesional.

También supone una garantía procesal fundamental en el sentido de que los medios de prueba han de ser obtenidos legalmente y nunca vulnerando derechos fundamentales[5].

El sujeto activo de este derecho es cualquier persona, bien individual, bien colectiva, bien nacional, bien extranjera, tanto viva, como fallecida. Y el sujeto pasivo es el estado, radicando tal carácter especialmente el poder ejecutivo y el poder judicial.

También es sujeto pasivo las personas individuales y los grupos sociales, religiosos, partidos políticos y todo aquel susceptible de ser violentado en este derecho.

Es especialmente subrayable la posición de sujeto pasivo, de las compañías o empresas que suministran los servicios telefónicos, por estar en una posición privilegiada desde el punto de vista técnico, de mayor posibilidad o facilidad de interceptación de las conversaciones telefónicas e incluso al ser un único proveedor, como es en el México actual, este privilegio es por demás incuestionable, por lo que es primordial el preguntarse si esta garantía es en verdad respetada.

El objeto o bien de la personalidad protegido es la intimidad o mas específicamente, los datos pertenecientes a la intimidad que son objeto de conversación telefónica.

---

[5] Para tales efectos, la legislación aplicable se refiere al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, así como el Código De Procedimientos Civiles Federal en el Titulo IV, de los artículos 79 al 218 .

También el objeto de protección es el anonimato de las personas que conversan.

Este derecho tiene relación muy directa con el derecho a la información. Son susceptibles de ser difundidas aquellas noticias obtenidas a través de escuchas telefónicas siempre que respondan a un interés general y no pertenezcan a la más estricta intimidad.

También existe una estrecha relación este derecho con el derecho al honor, pues las noticias o datos descubiertos a través de las escuchas telefónicas pueden suponer un grave atentado al buen nombre o fama de la persona.

También tienen una especial relación con este derecho todos los derechos referentes a la vida y seguridad personal y a la integridad psico-física de todos los ciudadanos en relación a las formas de actuación de la policía, especialmente en los países totalitarios, en los que son sistemáticamente vulneradas todo tipo de garantías penales del detenido.

En relación a las escuchas telefónicas realizadas por partidos políticos es importante también señalar la necesidad de su estricto control pues anda en juego la limpieza del funcionamiento democrático y pluralista de las instituciones.

Este derecho tiene relación muy directa con el derecho a la información. Son susceptibles de ser difundidas aquellas noticias obtenidas a través de escuchas telefónicas siempre que respondan a un interés general y no pertenezcan a la más estricta intimidad.

También existe una estrecha relación este derecho con el derecho al honor, pues las noticias o datos descubiertos a través de las escuchas telefónicas pueden suponer un grave atentado al buen nombre o fama de la persona.

El derecho a la intimidad frente a las escuchas telefónicas representa la síntesis de los problemas que se cuestionan en relación a la relación Estado- libertad individual, y más concretamente en la relación Poder Punitivo del Estado-libertad e intimidad individual.

Parece evidente que la intimidad debe ser una barrera infranqueable tanto por parte del Poder Publico -y por tanto del Poder punitivo-, como por parte de los particulares, pues en conexión directa con ella, reconocida como derecho fundamental, se encuentra la posibilidad de ejercicio de los demás derechos, así como de sus correspondientes garantías.

EL DERECHO A LA INTIMIDAD FRENTE A LA INFORMÁTICA: EL DERECHO A LA LIBERTAD INFORMÁTICA

En Enero de 1992 los medios de comunicación social dan la noticia de que ha sido descubierta la existencia de una red ilegal de venta de datos informatizados, cuyos bancos de datos contenían información de datos íntimos de muy variada índole, de veintiún millones de ciudadanos españoles. Los datos habían sido obtenidos ilegalmente de los Ministerios de la Presidencia, Interior, Trabajo y Hacienda.

Dada la enorme modernidad del derecho a la libertad informática, debida al acelerado avance tecnológico en materia informática, ninguno de los textos internacionales de Derechos Humanos hace referencia explícita de dicho derecho fundamental. Se puede entender sin embargo que este derecho puede reconocerse regulado implícitamente en los artículos de las principales

declaraciones internacionales que reconocen el derecho a la libertad, el derecho a la seguridad personal y el derecho a la intimidad, mencionados con anterioridad, esto aunado, como veremos mas adelante, a interesantes progresos en esta libertad en el campo informático–electrónico y sobre todo en beneficio del derecho informático.

EL DERECHO A LA LIBERTAD INFORMÁTICA.

El derecho a la libertad informática o derecho a la autodeterminación informática es un derecho fundamental de muy reciente aparición y pobremente tratado en nuestra legislación mexicana.

Está vinculado a la fuerte evolución tecnológica que ha experimentado la informática en los últimos veinte años. Lo cual ha permitido el almacenamiento, tratamiento y transmisión automatizada de una enorme cantidad de información personal.

La posibilidad de poder cruzar información procedente de distintas bases de datos ha multiplicado las posibilidades de lesión de los derechos de los ciudadanos a través de la informática

Podemos conceptuar El derecho a la libertad informática como aquel derecho fundamental de naturaleza autónoma, aunque derivado del genérico derecho a la intimidad, que asegura la identidad de las personas ante el riesgo de que sea invadida o expropiada a través del uso ilícito de las nuevas tecnologías, bien por parte del Estado, bien por parte de particulares.

Son sujetos activos de este derecho:

a) La persona individual.

b) La familia.

c) Los grupos sociales de todo tipo: religiosos, profesionales, culturales, minorías raciales.

El sujeto pasivo es el Estado y aquellos grupos sociales (como los grupos económicos) que pueden tener interés en conculcar el derecho a la libertad informática en beneficio propio, bien de una forma lucrativa, bien a través de la obtención de unos datos que les permiten aumentar su poder de dominación o de influencia.

Los bienes de la personalidad sobre los que recae la protección de la libertad informática son:

a) La intimidad, entendida, -como la entiende el Informe Younger sobre la intimidad, publicado en Inglaterra en Julio de 1972, en un doble sentido:[6]

b) La intimidad física, que supone "libertad frente a toda intromisión sobre uno mismo, su casa, su familia o relaciones".

[6] Facultad De Ciencias Jurídicas Y Sociales De La Universidad De Talca, Revista Jurídica Ius Et Praxis "DERECHO A LA AUTODETERMINACIÓN INFORMATIVA Y LA ACCIÓN DE HABEAS DATA EN IBEROAMERICA" Chile 1997 ,año 3 No. 1 pag 37

c) La intimidad informativa, que es "el derecho a determinar por uno mismo cómo y en qué medida se puede comunicar a otros información sobre uno mismo". Es la autodeterminación informativa de la propia intimidad.

d) La seguridad personal.

e) La libertad personal.

f) En general, todos los bienes de la personalidad que, en su caso, puedan verse afectados por la violación de este derecho.

El derecho a la libertad informática supone o implica el derecho a acceder y controlar, a través de las adecuadas vías procesales, las informaciones que les conciernen, procesadas en bancos de datos informatizados, el derecho a exigir de los bancos de datos públicos y privados la corrección de datos inexactos, el derecho a exigir de los bancos de datos públicos y privados el cancelar aquellos datos que resulten anticuados, inapropiados o irrelevantes, a exigir de los bancos de datos públicos y privados el cancelar aquellos datos personales que hayan sido obtenidos por procedimientos ilegales, a exigir que se tomen las medidas suficientes para garantizar la intimidad en relación a los datos estadísticos y a exigir que se tomen las medidas suficientes para evitar la transmisión de datos a personas o entidades no autorizadas.

Por otra parte tiene una clara conexión con el derecho a la participación política. Por su carácter público el derecho a la libertad informática "contribuye a conformar un orden político basado en la equilibrada participación cívica y colectiva en los procesos de información y comunicación que definen el ejercicio del poder en las "sociedades informatizadas" de nuestra época"

La libertad informática o autodeterminación informativa es la necesaria respuesta al fenómeno de la "contaminación de las libertades" en los sistemas jurídicos democráticos, debida al desajuste o desfase existente entre las lentas normas jurídicas y el consiguiente desarrollo de las garantías de los derechos fundamentales y por otra parte, del vertiginoso avance tecnológico.

En los sistemas totalitarios se hace aún más necesario la protección de los particulares frente al poder del Estado pues éste tiene en la informática, y en otras formas del poder tecnológico un asociado potentísimo, de muy difícil control por parte de los ciudadanos.

En los sistemas democráticos se hace preciso un estricto control sobre los bancos de datos que obran en poder de los órganos del Estado. Y ello como garantía tanto frente a la actuación por parte del Estado, como frente a la actuación de los particulares. Téngase en cuenta que esos datos confidenciales, sin un control adecuado, pueden ser utilizados peligrosamente en el mercado de trabajo (aplicación de criterios discriminatorios por razones de raza, de creencias, etc) o en otros aspectos de la vida social que pueden llegar a ser extremadamente perversos y atentatorios contra los Derechos Humanos.

1.1.1- ANTECEDENTES SOBRE EL DERECHO A LA INTIMIDAD.

El primer antecedente conocido sobre el derecho a la Intimidad, aunque ha tomado mas auge en la actualidad, está en Declaración De Derechos De Virginia Del 12 De Junio De 1776, misma que estipula en su cuerpo, aunque de manera implícita, en su articulo 10 que "las ordenes judiciales, por medio de las cuales un funcionario o agente puede allanar un sitio sospechoso sin prueba de hecho cometido, o arrestar a cualquier persona o personas no mencionadas, o cuyo delito no está especialmente descrito o probado, son opresivas y crueles, y no deben ser extendidas."Mas en un ámbito mas cercano a Nuestro Sistema Jurídico, este aparece mas concatenado con la declaración de los derechos del

hombre y el ciudadano de 1789 de forma implícita en el cuerpo de esa declaración, al observarse en la misma como garantía de seguridad jurídica en amplio sentido, protegiendo a sus gobernados, pero la abstracción que surge al interpretarlo en cuanto al derecho a la intimidad, es con respecto al proteger los bienes y personas de las personas.

Así, a través de la historia, siempre ha existido la preocupación de proteger al hombre de los abusos y arbitrariedades cometidos en su contra por parte de la autoridad.

Los Derechos Humanos se han constituido en una conciencia moral de la humanidad y en consecuencia no pueden ser abolidos, sino únicamente pueden y deben ser respetados y defendidos con la certeza de su pleno conocimiento.

Pero tan cambiante como es nuestra ciencia, es imposible que esta misma se vaya rezagando con la misma, por lo que al considerar el derecho a la intimidad como parte integrante de los derechos humanos, es necesario estudiar su evolución en conjunción con las demás.

Por lo que en la en la evolución histórica de los Derechos Humanos existen varias etapas, que son clasificadas de la siguiente forma:

PRIMERA ETAPA .- Del siglo XVIII a.C. al siglo V d.C., la problemática de los valores del ser humano, se ve reflejada en algunos documentos normativos, como el Código de Hammurabi, en Babilonia, ordenamiento jurídico de cierto contenido social que establecía límites a la esclavitud por deudas y regulaba precios, entre otras cosas. En la misma época, aparece el Decálogo, que tenía como finalidad la protección de la dignidad humana, al prohibir el homicidio, equivalente a la protección a la vida.

SEGUNDA ETAPA.- Del siglo V al siglo XV d.C., domina la filosofía del cristianismo sobre cualquier otra ideología, dando lugar al humanismo cristiano. Se habla de un derecho natural divino, donde destacan las ideas de San Agustín y Santo Tomás de Aquino.

Los Derechos Humanos, son perfilados con sentido comunitario. Ejemplo de ello es la llamada Carta Magna de Juan Sin Tierra en el año de 1215, que contempla algunas garantías como la de seguridad jurídica, restringiéndose el poder del monarca. Simultáneamente, en España aparecen los ordenamientos legales llamados "fueros", que consistían en la capacidad de cada pueblo para regirse conforme a sus propias leyes.

TERCERA ETAPA.- Del siglo XV al siglo XVI!, se consolidan en Inglaterra algunas libertades a pesar de las grandes monarquías, como reacción a esta forma de gobierno mediante reclamaciones de libertad en el campo de las creencias, plasmándose en ordenamientos legales los Derechos Humanos como límite a la acción gubernamental. En esta época, se postula la existencia de una serie de derechos y libertades frente al monarca, aceptados por el pueblo como inderogables. Un ejemplo es la importancia que se le dió a los valores de libertad, propiedad e igualdad.

CUARTA ETAPA.- Comprende los siglos XVIII y XIX, época donde surgen movimientos revolucionarios, iniciados en Francia, sirviendo de ejemplo a otros países en Europa y América, originándose las luchas independentistas, de las que resultaron las naciones americanas.

En el Continente Americano, los Derechos Humanos tienen su origen en la Declaración de Derechos de Virginia en 1714, que se consolidan mediante la

Declaración Francesa de los Derechos del Hombre y el Ciudadano en el año de 1789, documento en el que se plasman las ideas de la Revolución Francesa.

En la declaración francesa, por primera vez se establecen los Derechos Humanos como pertenecientes al hombre por el hecho de ser hombre; estos derechos adquieren el carácter de universales y se incorporan a las constituciones nacionales.

QUINTA ETAPA.- Abarca el siglo XX, durante la cual numerosas constituciones amplían su ámbito, incluyendo los derechos económicos, sociales y culturales. Un ejemplo es la Constitución Política de los Estados Unidos Mexicanos, que sentó las bases para que en el plano internacional se incorporaran los Derechos Humanos, caracterizándose su evolución después de la Segunda Guerra Mundial, con el nacimiento de diversos tratados y convenios multinacionales entre los que destacan los siguientes:

A) La Declaración Americana de Derechos y Deberes del Hombre de la O.E.A. (1948).

B) La Declaración Universal de Derechos Humanos, adoptada en el marco de la O.N.U. (10 Dic. 1948).

C) Los Pactos de Derechos Civiles y Políticos; Derechos Económicos, Sociales y Culturales, ambos de la O.N.U. (1966).

D) La Convención Europea para la Protección de los Derechos Humanos y Libertades Fundamentales (1950).

E) La Convención Americana de los Derechos Humanos: Pacto de San José de la O.E.A. (1969).

Durante esta época, se desarrolla un sistema de protección de los Derechos Humanos a nivel internacional, con procedimientos y órganos especiales encargados de velar por el fiel cumplimiento de las obligaciones contraídas internacionalmente por los países.

EVOLUCIÓN HISTÓRICA A NIVEL NACIONAL

En la época colonial se vivió un sistema jurídico estamentario, el cual consistía en la impartición de justicia de acuerdo a la condición social, económica, religiosa o militar del individuo, por lo que se reconocían derechos mínimos a la clase baja, y a la clase alta se le otorgaban mayores derechos en proporción a su posición social.

La influencia del pensamiento enciclopedista de Europa, se hizo presente en nuestro país, mediante la obra de Fray Bartolomé de las Casas (El Memorial 1562/1563), en la que se condenan la conquista, la guerra, la violencia, la opresión y se justifica la rebelión de los indígenas, defendiendo su dignidad, libertad e igualdad.

Paralelamente en Europa se desarrollaron las estructuras sociales y políticas, así como las económicas. Las ideas de Hobbes, Locke, Rousseau y Montesquieu, fundamentan el nacionalismo del siglo XIX, que posteriormente se introducen en nuestro país por medio de Alejandro de Humboldt.

Factores importantes en la Independencia de México, fueron: la Declaración de Independencia de los Estados Unidos (1776) y la Declaración de los Derechos del Hombre y del Ciudadano de Francia (1789).

Así, mientras que a nivel internacional se inicia la normatividad de los Derechos Humanos sobre el individuo y la sociedad haciéndolos ley, en México se avanza hacia la Independencia.

Antes de la Constitución que nos rige, se elaboraron diversos documentos que contemplaron los Derechos Humanos. Durante el México Insurgente y la etapa Independiente del siglo pasado, surgieron como ejemplos las constituciones de 1814, 1824 y 1857, siendo la de 1917, la primera en el mundo con espíritu social.

El espíritu de esta evolución se ve plasmado en varios artículos de nuestra Carta Magna, Base principal es el Articulo 16 constitucional que en su cuerpo contempla"

"Las comunicaciones privadas son inviolables. La Ley sancionará plenamente cualquier acto que atente contra la libertad y privacía 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. Para ello, la autoridad competente, por escrito, deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor."

"Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes. Los resultados de las intervenciones que no cumplan con éstos, 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."

1.2.- HISTORIA DE LA INFORMÁTICA Y EL DERECHO INFORMÁTICO.

La Computación, y por tanto, las Ciencias de la Computación y con ello la informática, tienen su origen en el cálculo, es decir, en la preocupación del ser humano por encontrar maneras de realizar operaciones matemáticas de forma cada vez más rápida y más fácilmente. Pronto se vio que con ayuda de aparatos y máquinas las operaciones podían realizarse de forma más rápida y automática.

El primer ejemplo que encontramos en la historia es el ábaco, aparecido hacia el 500 AC en Oriente Próximo, que servía para agilizar las operaciones aritméticas básicas, y que se extendió a China y Japón, siendo descubierto mucho más tarde por Europa.

También es digno de señalar el conocido Mecanismo de Antikythera, recuperado en 1900, construido alrededor del año 80 A.C., en la isla griega de Rodas, ubicada en el mar Egeo. Era un artefacto de cálculo astronómico con mecanismos de precisión. El usuario, por medio de una perilla, podía accionar un simulador en miniatura del movimiento del sol, la luna y varios planetas, teniendo a la vista la fecha en que se había dado, o se daría, tal combinación. Es tanta su sofisticación que ha sido llamado la primera computadora de Occidente.

Por otra parte, los matemáticos hindúes, árabes y europeos fueron los primeros que desarrollaron técnicas de cálculo escrito. El matemático árabe Al'Khwarizmi, alrededor del año 830 DC, escribe un libro de Aritmética, traducido al latín como Algoritmi de numero Indorum, donde introduce el

sistema numérico indio (sólo conocido por los árabes unos 50 años antes) y los métodos para calcular con él. De esta versión latina proviene la palabra algoritmo.

A finales del siglo XVI y comienzos del XVII comienza lo que denominamos Era Mecánica, en la que se intenta que aparatos mecánicos realicen operaciones matemáticas de forma prácticamente automática. En 1610, John Napier (1550-1617), inventor de los logaritmos, desarrolló las Varillas de Napier, que servían para simplificar la multiplicación. En 1641, el matemático y filósofo francés Blaise Pascal (1623-1662), con tan sólo 19 años, construyó una máquina mecánica para realizar adiciones, la Pascalina, para ayudar a su padre. Por su parte, Gottfried Wilhelm Leibniz (1646-1716) propuso el sistema binario para realizar los cálculos, construyendo una máquina que podía multiplicar, en incluso teóricamente, realizar las cuatro operaciones aritméticas. Sin embargo, la tecnología disponible le imposibilita la realización de las operaciones con exactitud. No obstante un estudiante alemán de la Universidad de Tubingen, Wilhelm Schickard (1592-1635) ya había construido una máquina de estas características entre 1623 y 1624, de la que hace unas breves descripciones en dos cartas dirigidas a Johannes Kepler. Por desgracia, al menos una de las máquinas quedó destruida en un incendio, y el propio Schickard murió poco después, víctima de la peste bubónica.

Los trabajos de Pascal y Leibniz tuvieron su continuación en 1727, cuando Jacob Leupold propuso algunas mejoras sobre el mecanismo de Leibniz. En 1777, Charles Mahon (1753-1816), Conde de Stanhope, construyó una máquina aritmética y otra lógica, esta última llamada Demostrador de Stanhope. En 1825, el francés Charles Xavier Thomas de Colmar diseña una máquina calculadora que posteriormente consigue comercializar con éxito.

Una mención muy especial requiere el desarrollo de un telar automático por el francés Joseph Jacquard (1752-1834), en 1801. En efecto, analizando las operaciones repetitivas que requería la producción de telas, este inventor imaginó conservar la información repetitiva necesaria bajo la forma de perforaciones en tarjetas. Estas perforaciones eran detectadas mecánicamente, asegurando el desplazamiento adecuado de las guías del hilado, pudiendo una sola persona tejer complicados patrones codificados en las perforaciones de las tarjetas.

Fue Charles Babbage (1791-18171) el que diseñó una verdadera máquina procesadora de información, capaz de autocontrolar su funcionamiento. Desesperado por los errores contenidos en las tablas numéricas de la época y dándose cuenta de que la mayoría de los cálculos consistían en tediosas operaciones repetitivas, este profesor de la Universidad de Cambridge, proyecta e inicia la construcción de un nuevo tipo de calculadora. En 1821 presentó a la Royal Society una máquina capaz de resolver ecuaciones polinómicas mediante el cálculo de diferencias sucesivas entre conjuntos de números, llamada Máquina Diferencial. Obtuvo por ello la medalla de oro de la Sociedad en 1822.

Más tarde, Babbage empezó a trabajar en la Máquina Analítica, en cuya concepción colaboró directamente Ada Augusta Byron, Condesa de Lovelace, hija de Lord Byron. El objetivo perseguido era obtener una máquina calculadora de propósito general, controlada por una secuencia de instrucciones, con una unidad de proceso, una memoria central, facilidades de entrada y salida de datos, y posibilidades de control paso a paso, es decir, lo que hoy conocemos como programa. Ada Lovelace, a quien se reconoce como la primera programadora de la historia, y en honor de quien se puso el nombre de Ada al conocido lenguaje de programación, ayudó a Babbage económicamente, vendiendo todas sus joyas, y escribió artículos y programas para la referida

máquina, algunos de ellos sobre juegos. Sin embargo, este proyecto tampoco pudo realizarse por razones económicas y tecnológicas.

En el 1854, George Boole publica Las leyes del pensamiento sobre las cuales son basadas las teorías matemáticas de Lógica y Probabilidad. Boole aproximó la lógica en una nueva dirección reduciéndola a un álgebra simple, incorporando lógica en las matemáticas. Comenzaba el álgebra de la lógica llamada Álgebra Booleana. Su álgebra consiste en un método para resolver problemas de lógica que recurre solamente a los valores binarios 1 y 0 y a tres operadores: AND (y), OR (o) y NOT (no).

A partir de este momento, se inicio la llamada evolución generacional, dividiéndose de esta forma:

LA PRIMERA GENERACIÓN (ELECTROMECÁNICOS Y ELECTRÓNICOS DE TUBOS DE VACÍO).-Para tabular el censo de 1890, el gobierno de Estados Unidos estimó que se invertirían alrededor de diez años. Un poco antes, Herman Hollerith (1860-1929), había desarrollado un sistema de tarjetas perforadas eléctrico y basado en la lógica de Boole, aplicándolo a una máquina tabuladora de su invención. La máquina de Hollerith se usó para tabular el censo de aquel año, durando el proceso total no más de dos años y medio. Así, en 1896, Hollerith crea la Tabulating Machine Company con la que pretendía comercializar su máquina. La fusión de esta empresa con otras dos, dio lugar, en 1924, a la International Business Machines Corporation (IBM).

Sin embargo, en el censo de 1910, el sistema de Hollerith fue sustituido por uno desarrollado por James Powers. En 1911 James Powers constituyó la Power's Tabulating Machine Company, convirtiéndose en el principal competidor de Hollerith.

En 1900, en el Congreso Internacional de Matemáticas de París, David Hilbert (1862-1943) pronunció una conferencia de título Problemas matemáticos, en la que proponía una lista de 23 problemas que estaban sin resolver.

En 1936, Alan Turing (1912-1954) contestó a esta cuestión en el artículo On Computable Numbers. Para resolver la cuestión Turing construyó un modelo formal de computador, la Máquina de Turing, y demostró que había problemas tales que una máquina no podía resolver. Al mismo tiempo en Estados Unidos contestaba a la misma cuestión Alonzo Chuch, basándose en una notación formal, que denominó cálculo lambda, para transformar todas las fórmulas matemáticas a una forma estándar. Basándose en estos resultados, entre 1936 y 1941, el ingeniero alemán Konrad Zuse (1910-1957), diseñó y construyó su serie de computadores electromecánicos binarios, desde el Z1 hasta el Z3. Sin embargo estos computadores no tuvieron mucha difusión, ni siquiera dentro de su país, ya que el gobierno nazi nunca confió en los trabajos de Zuse.

En 1938, Claude Shannon demostró cómo las operaciones booleanas elementales, se podían representar mediante circuitos conmutadores eléctricos, y cómo la combinación de circuitos podía representar operaciones aritméticas y lógicas complejas. Además demostró como el álgebra de Boole se podía utilizar para simplificar circuitos conmutadores. El enlace entre lógica y electrónica estaba establecido.

Al desencadenarse la Segunda Guerra Mundial, la necesidad de realizar complicados cálculos balísticos y la exigencia de descodificar los mensajes cifrados del otro bando, impulsó el desarrollo de los computadores electrónicos de propósito general. El propio Turing fue reclutado en Bletchley Park, en Inglaterra, para descifrar los mensajes que encriptaba la máquina alemana Enigma, para lo que fue necesario construir la computadora Colossus.

En la Universidad de Harvard, Howard Aiken (1900-1973) en colaboración con IBM, empezó, en 1939, la construcción del computador electromecánico Mark I, en la que trabajó como programadora Grace Murray Hopper. Pero para cuando se terminó en 1944, ya habían aparecido las primeras computadoras totalmente electrónicas, que eran mucho más rápidas.

Por otro lado, en la Universidad del Estado de Iowa, entre 1937 y 1942, John Vincent Atanasoff (1903-1995) y Clifford Berry, diseñaron y construyeron la ABC (Atanasoff-Berry Computer). Terminada en 1942, fue la primera computadora electrónica digital, aunque sin buenos resultados y nunca fue mejorada. En 1941, John W. Mauchly (1907-1980) visitó a Atanasoff y observó de cerca su impresionante maquinaria, teniendo la oportunidad de revisar su tecnología. Más tarde, Mauchly y J. Presper Eckert, Jr (1919-1995), diseñaron y construyeron, entre los años 1943 y 1946, el computador eléctrico de propósito general ENIAC. Existe una gran controversia respecto a que Mauchly copiara muchas de las ideas y conceptos del profesor Atanasoff, para construir la computadora ENIAC. En cualquier caso en las últimas fases de su diseño y construcción aparece la importante figura de John Von Neumann (1903-1957), que actúa como consultor.

Von Neumann escribió en 1946, en colaboración con Arthur W. Burks y Herman H. Goldstine, Preliminary Discussion of the Logical Design of an Electronic Computing Instrument, que contiene la idea de Máquina de Von Neumann, que es la descripción de la arquitectura que, desde 1946, se aplica a todos los computadores que se han construido.

Con estos fundamentos, Eckert y Mauchly construyen en la Universidad de Manchester, en Connecticut (EE.UU.), en 1949 el primer equipo con capacidad de almacenamiento de memoria, la EDVAC. Eckert y Mauchly forman una corporación para construir una máquina que se pueda comercializar, pero,

debido a problemas financieros, se vieron obligados a vender su compañía a a Remington Rand Corp. Trabajando para esta compañía fue que se concluyó el proyecto Univac, en 1951.

También por esta época Maurice Wilkes construye la EDSAC en Cambridge (Inglaterra) y F.C. Williams construye en Manchester (Inglaterra), la Manchester Mark I.

Estas máquinas se programaban directamente en lenguaje máquina, pero a partir de mediados de los 50, se produjo un gran avance en la programación avanzada.

LA SEGUNDA GENERACIÓN (LOS TRANSISTORES Y LOS AVANCES EN PROGRAMACIÓN).- Allá por 1945 la máxima limitación de las computadoras era la lenta velocidad de procesamiento de los relés electromecánicos y la pobre disipación de calor de los amplificadores basados en tubos de vacío.

En 1947, John Bardeen, Walter Brattain y William Shockley inventan el transistor, recibiendo el Premio Nobel de Física en 1956. Un transistor contiene un material semiconductor, normalmente silicio, que puede cambiar su estado eléctrico. En su estado normal el semiconductor no es conductivo, pero cuando se le aplica un determinado voltaje se convierte en conductivo y la corriente eléctrica fluye a través de éste, funcionando como un interruptor electrónico.

Los computadores construidos con transistores eran más rápidos, más pequeños y producían menos calor, dando también oportunidad a que, más tarde, se desarrollaran los microprocesadores. Algunas de las máquinas que se construyeron en esta época fueron la TRADIC, de los Laboratorios Bell (donde se inventó el transistor), en 1954, la TX-0 del laboratorio LINCOLN del MIT y las IBM 704, 709 y 7094. También aparece en esta generación el concepto de

supercomputador, específicamente diseñados para el cálculo en aplicaciones científicas y mucho más potentes que los de su misma generación, como el Livermore Atomic Research Computer (LARC) y la IBM 7030.

Pero esta generación se explica también por los avances teóricos que se dan.

Así, en 1950, Alan Turing publica el artículo Computing Machinery and Intelligence en la revista Mind, en el que introducía el célebre Test de Turing. Este artículo estimuló a los pensadores sobre la filosofía e investigación en el campo de la Inteligencia Artificial. Por desgracia, Turing no fue testigo del interés que desató su artículo, porque en 1952 fue detenido por su relación homosexual con Arnold Murray y fue obligado a mantener un tratamiento con estrógenos que le hizo impotente y le produjo el crecimiento de pechos. En 1957, fue encontrado muerto en su casa al lado de una manzana mordida a la que había inyectado cianuro.

En 1951, Grace Murray Hooper (1906-1992) da la primera noción de compilador y más tarde desarrolla el COBOL. Pero fue John Backus, en 1957, el que desarrolla el primer compilador para FORTRAN. En 1958, John MacCarthy propone el LISP, un lenguaje orientado a la realización de aplicaciones en el ámbito de la Inteligencia Artificial. Casi de forma paralela, Alan Perlis, John Backus y Peter Naur desarrollan el lenguaje ALGOL.

Pero el personaje más importante en el avance del campo de los algoritmos y su análisis, es Edsger Dijkstra (1930-), que en 1956, propuso su conocido algoritmo para la determinación de los caminos mínimos en un grafo, y más adelante, el algoritmo del árbol generador minimal. Más tarde, en 1961, N. Brujin introduce la notación O, que sería sistematizada y generalizada por D. Knuth. En 1957, aparece la Programación Dinámica de la mano de R. Bellman.

En 1960, S. Golomb y L. Baumet presentan las Técnicas Backtracking para la exploración de grafos. Se publican en 1962 los primeros algoritmos del tipo Divide y Vencerás: el QuickSort de Charles Hoare y el de la multiplicación de grandes enteros de A. Karatsuba e Y. Ofman.

En 1959, Jack Kilby (1923-) presenta el primer circuito integrado, un conjunto de transistores interconectados con resistencias, en una pequeña pastilla de silicio y metal, llamada chip. Fue a partir de este hecho que las computadoras empezaron a fabricarse de menor tamaño, más veloces y a menor costo, debido a que la cantidad de transistores colocados en un solo chip fue aumentando en forma exponencial.

TERCERA GENERACIÓN (CIRCUITOS INTEGRADOS Y MINITUARIZACIÓN).- A partir del circuito integrado, se producen nuevas máquinas, mucho más pequeñas y rápidas que las anteriores, así aparecen las IBM 360/91, IBM 195, SOLOMON (desarrollada por la Westinghouse Corporation) y la ILLIAC IV, producida por Burroughs, el Ministerio de Defensa de los EE.UU y la Universidad de Illinois.

Seymour Cray (1925-1996) revoluciona el campo de la supercomputación con sus diseños: en 1964, el CDC 6600, que era capaz de realizar un millón de operaciones en coma flotante por segundo; en 1969, el CDC 7600, el primer procesador vectorial, diez veces más rápido que su predecesor.

En cuanto a los avances teóricos, a mediados de los 60, un profesor de Ciencias de la Computación, Niklaus Wirth, desarrolla el lenguaje PASCAL, y en Berkeley, el profesor Lotfi A. Zadeh, publica su artículo Fuzzy Sets, que revoluciona campos como la Inteligencia Artificial, la Teoría de Control o la Arquitectura de Computadores.

En 1971, Intel introduce el primer microprocesador. El potentísimo 4004 procesaba 4 bits de datos a la vez, tenía su propia unidad lógico aritmética, su propia unidad de control y 2 chips de memoria. Este conjunto de 2.300 transistores que ejecutaba 60.000 operaciones por segundo se puso a la venta por 200 dólares. Muy pronto Intel comercializó el 8008, capaz de procesar el doble de datos que su antecesor y que inundó los aparatos de aeropuertos, restaurantes, salones recreativos, hospitales, gasolineras, entre otros.

A partir de aquí nacieron las tecnologías de integración a gran escala (LSI) y de integración a muy gran escala (VLSI), con las que procesadores muy complejos podían colocarse en un pequeño chip.

Sin embargo, hasta este momento, por motivos económicos, complejidad de uso y dificultad de mantenimiento, los computadores habían sido patrimonio de universidades, organismos militares y gubernamentales, y grandes empresas.

En 1975, Popular Electronics dedicó su portada al primer microcomputador del mundo capaz de rivalizar con los modelos comerciales, el Altair 8800.

CUARTA GENERACIÓN (ORDENADORES PERSONALES DE USO DOMÉSTICO).- El Altair 8800, producido por una compañía llamada Micro Instrumentation and Telemetry Systems (MITS), se vendía a 397 dólares, lo que indudablemente contribuyó a su popularización. No obstante, el Altair requería elevados conocimientos de programación, tenía 256 bytes de memoria y empleaba lenguaje máquina. Dos jóvenes, William Gates y Paul Allen, ofrecieron al dueño de MITS, un software en BASIC que podía correr en el Altair. El software fue un éxito y, posteriormente Allen y Gates crearon Microsoft.

Paralelamente, Steven Wozniak y Steven Jobs, también a raíz de ver el Altair 8800 en la portada de Popular Electronics, construyen en 1976, la Apple I. Steven Jobs con una visión futurista presionó a Wozniak para tratar de vender el modelo y el 1 de Abril de 1976 nació Apple Computer. En 1977, con el lanzamiento de la Apple II, el primer computador con gráficos a color y carcasa de plástico, la compañía empezó a imponerse en el mercado.

En 1981, IBM estrena una nueva máquina, la IBM Personal Computer, protagonista absoluta de una nueva estrategia: entrar en los hogares. El corazón de esta pequeña computadora, con 16 Kb de memoria (ampliable a 256), era un procesador Intel, y su sistema operativo procedía de una empresa recién nacida llamada Microsoft.

En 1984, Apple lanza el Macintosh, que disponía de interfaz gráfico para el usuario y un ratón, que se hizo muy popular por su facilidad de uso.

QUINTA GENERACIÓN.- En vista de la acelerada marcha de la microelectrónica, la sociedad industrial se ha dado a la tarea de poner también a esa altura el desarrollo del software y los sistemas con que se manejan las computadoras. Surge la competencia internacional por el dominio del mercado de la computación, en la que se perfilan dos líderes que, sin embargo, no han podido alcanzar el nivel que se desea: la capacidad de comunicarse con la computadora en un lenguaje más cotidiano y no a través de códigos o lenguajes de control especializados.

Japón lanzó en 1983 el llamado "programa de la quinta generación de computadoras", con los objetivos explícitos de producir máquinas con innovaciones reales en los criterios mencionados. Y en los Estados Unidos ya

está en actividad un programa en desarrollo que persigue objetivos semejantes, que pueden resumirse de la siguiente manera:

a) Procesamiento en paralelo mediante arquitecturas y diseños especiales y circuitos de gran velocidad.

b) Manejo de lenguaje natural y sistemas de inteligencia artificial.

Actualmente se encuentra en desarrollo la llamada sexta generación, misma que basa su funcionamiento básico en operaciones quánticas y el desarrollo de la operaciones lógico matemáticas, en el contorno de un funcionamiento en base al DNA(ácido desoxirribunucleico, estructura que en lugar de usar el sistema binario(basado en el uso del 0 y el uno para la constitución de números) utiliza un sistema cuádruple mediante operadores lógicos(OR, NOT , IF Y OR NOT).

El futuro previsible de la computación es muy interesante, y se puede esperar que esta ciencia siga siendo objeto de atención prioritaria de gobiernos y de la sociedad en conjunto.

1.2. HISTORIA DEL DERECHO INFORMÁTICO

De reciente aparición en la historia del hombre, el surgimiento del tal rama del derecho la podemos considerar a partir del momento en que la gente empezó a correlacionarse a través de la computadora, compartiendo e intercambiando información, y como sucede, viene consigo la aparición de actos jurídicos, muchos de ellos no regulados en la actualidad.

Esta rama, en la que aun hay grandes divergencias para encuadrarla [7] podemos definirla como "el sector normativo de los sistemas, dirigido a la regulación de las nuevas tecnologías de la información y la comunicación, es decir, la informática y la telemática[8]".

Asimismo integran el Derecho Informático las proposiciones normativas, es decir, los razonamientos de los teóricos del Derecho que tienen por objeto analizar, interpretar, exponer, sistematizar o criticar el sector normativo que disciplina la informática y la telemática. Las fuentes y estructura temática del Derecho Informático afectan las ramas del Derecho Tradicionales.

Además, se inscriben en el ámbito del Derecho Público: El problema de la regulación del flujo internacional de datos informatizados, que interesa al derecho internacional público; la Libertad Informática, o defensa de las libertades frente a eventuales agresiones perpetradas por las tecnologías de la información y la comunicación, objeto de especial atención por parte del Derecho Constitucional y Administrativo; o los delitos informáticos, que tienden a configurar un ámbito propio en el Derecho Penal Actual. Mientras que inciden directamente en el Ámbito del Derecho Privado cuestiones, tales como: Los contratos informáticos, que pueden afectar lo mismo al hardware que al software, dando lugar a una rica tipología de los negocios en la que pueden distinguirse contratos de compraventa, alquiler, leasing[9], copropiedad, multicontratos de compraventa, mantenimiento y servicios; como los distintos

---

[7] Leasing es el contrato de arrendamiento financiero por lo que"el arrendamiento financiero constituye un negocio jurídico de naturaleza crediticia, una técnica de financiamiento aplicada a la adquisición de bienes de equipo como a la construcción de inmuebles" LEON SOYLA, EL ARRENDAMIENTO FINANCIERO(LEASING) EN EL DERECHO MEXICANO, México UNAM 1989, pp.172 y 88

[8] Informática tiene una concepción muy general, tomaremos básicamente la noción de información que refiere el maestro Julio Téllez Valdes "como un proceso físico-mecánico de datos, teniendo como dato al elemento referencial de un hecho" Pág. 42 mientras que la telemática o la teleinformática el modo de transmitir mediante las telecomunicaciones y "permite asimilar más atingentemente al planeta como un verdadero mercado único de productos y servicios"pag 57 TELLEZ VALDES JULIO,"DERECHO INFORMÁTICO" UNAM, México,1991.

[9] LEON SOYLA, Ibidem, pag. 88

sistemas para la protección jurídica de los objetos tradicionales de los Derechos Civiles y Mercantiles.

Ese mismo carácter inter disciplinario o "espíritu transversal", que distingue al derecho informático, ha suscitado un debate teórico sobre: si se trata de un sector de normas dispersas pertenecientes a diferentes disciplinas jurídicas o constituye un conjunto unitario de normas (fuentes), dirigidas a regular un objeto bien delimitado, que se enfoca desde una metodología propia, en cuyo supuesto entraría una disciplina jurídica autónoma.

1.3.- MARCO HISTÓRICO DE LA RED "INTERNET" Y SU DESARROLLO.

La Internet ha significado una revolución sin precedentes en el mundo de la informática y de las comunicaciones y que ha transformado a la humanidad. Han contribuido a ello los inventos del teléfono, la radio, los satélites, las computadoras, dispositivos de hardware, los protocolos o estándares de comunicaciones y software especializados, tales como navegadores, correo electrónico, FTP, video conferencias, etc.

El 4 de Octubre de 1957 la antigua Unión Soviética puso en órbita el primer satélite artificial, llamado SPUTNIK, adelantándose a los Estados Unidos de América que 2 años antes había anunciado el inicio de una carrera inter espacial.

Este importante hecho marca el comienzo del uso de las comunicaciones globales. Un año después el presidente Dwight Eisenhower ordenó la creación de la Advanced Research Projects Agency (ARPA por sus siglas en ingles, Agencia De Proyectos De Investigación Avanzados, en español) creado por el Departamento de Defensa de los EUA así como la NASA.

1961 El Director del Defense Research and Engineering (DDR&E por sus siglas en ingles) asigna las funciones del ARPA.

Pasaron 5 años y en lo que se llamó la época de la Guerra Fría entre las más grandes potencias del mundo.

El gobierno de los Estados Unidos encargó en Octubre de 1962 a JCR Licklider, del Massachusetts Institute of Technology (MIT por sus siglas en ingles) que liderase a un grupo de investigadores y científicos para emprender el proyecto, ARPA, con fines de proteccionismo bélico en la eventualidad de un conflicto mundial.

La primera descripción documentada está contenida en una serie de memorándums escritos por J.C.R. Licklider, en Agosto de 1962, en los cuales expone 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 la información y los programas. En esencia, el concepto era muy parecido a la Internet actual. Licklider fue el principal responsable del programa de investigación en computadores de la DARPA desde Octubre de 1962. Mientras trabajó en ARPA 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. Entre 1962 y 1968 se trabajó el concepto de intercambio de paquetes, desarrollado por Leonard Kleintock y su origen y uso fue meramente militar. La idea consistía en que varios paquetes de información pudiesen tomar diferentes rutas para uno o más determinados destinos, consiguiendo con ello una mejor seguridad en el trasporte de la información. Se siguieron conectando computadores rápidamente a la ARPANET durante los años siguientes 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). 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.

En Septiembre de 1972, Ray Tomlinson, de BBN (Bolt, Beranek and Newman), escribió el software SENDMSG, 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 Octubre de 1972, Kahn organizó una gran y muy exitosa demostración de ARPANET en la International Computer Communication Conference(Conferencia de Comunicación por computadorao ICCC por sus siglas en ingles). 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 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.

A fines de 1972 el ARPANET fue renombrado como DARPANET (The Defense Advanced Research Projects Agency por sus siglas en ingles O La Agencia de proyectos de Investigación de Defensa Avanzada).

En 1973 se empezó el desarrollo del protocolo que más tarde se llamaría TCP/IP desarrollado por Vinton Cerf de la Universidad de Standford.

En 1976 el Dr. Robert M. Metcalfe desarrolla Ethernet, cuyo sistema permite el uso de cables coaxiales que permiten transportan la información en forma más rápida.

En 1976 es cuando recién DARPANET empieza a usar el protocolo TCP/IP

Ese mismo año se crea en los Laboratorios de la Bell de AT&T el UUCP (Unix to Unix Copy) distribuido con UNIX un año más tarde.

En 1979 se crea USENET, una red para intercambio de noticias grupales, y que fuera creado por Steven Bellovin y los programadores Tom Truscott y Jim Ellis, bajo la tecnología de UUCP.

En 1979 IBM crea BITNET (Because it is Time Network) que sirve para mensajes de correo y listas de interés.

En 1981 La National Science Foundation crea una red de comunicaciones llamada CSNET que transmite a 56 kbps, sin necesidad de acceder a ARPANET y es en este año que se empieza a independizar el control científico civil del control militar.

En 1983 se crea el Internet Activities Board. Para Enero de ese año todos los equipos conectados a ARPANET tenían que usar el protocolo TCP/IP que reemplazó al NCP, por completo.

La Universidad de Winsconsin creó el Domain Name System (DNS) que permitía dirigir los paquetes de datos a un nombre de dominio, cuyo servidor se encargaría de traducir la correspondiente dirección IP de cada equipo.

En 1984 la ARPANET se dividió en 2 redes centrales: MILNET Y ARPANET. La primera era de uso estrictamente militar y la segunda servía para mantener la investigación científica. Sin embargo el Departamento de Defensa de los EUA seguía controlando ambas.

En 1985-86: La National Science Foundation (NSF) conectó seis centros de super computación a través del país. Esta red es llamada la NSFNET, o sea la troncal (backbone) de la NSF.

Para expandir el acceso a Internet, la NSF auspició el desarrollo de redes regionales, las cuales fueron conectadas al troncal de la NSFNET. Sumándolo a esto la NSF apoyó a instituciones, tales como universidades y centros de investigación, en sus esfuerzos para conectarse a las redes regionales.

En 1987 - La NSF otorgó una concesión a Merit Network,Inc., para operar y administrar futuros desarrollos de la troncal de la NSFNET. Merit Network Inc. en una asociación con IBM, Corp. y con MCI Telecomunications, emprendieron investigaciones para el rápido desarrollo de nuevas tecnologías para redes.

En 1989 - La troncal de la red es elevada a "T1", con ello la red queda habilitada para trasmitir datos de hasta 1.5 millones de bits por segundo, o lo que es lo mismo hasta 50 páginas de texto por segundo.

En 1990 - La ARPANET es disuelta.

En 1991 - El Gopher es creado por la Universidad de Minnesota. El Gopher provee al usuario de un método basado en un menú jerárquico, que es capaz de localizar información en la Internet. Esta herramienta facilita enormemente el uso de la Internet.

En 1992 Se funda la Internet Society.

En 1993 - El European Laboratory for Particle Physics in Switzerland (CERN) libera el World Wide Web (WWW), desarrollado por Tim Berners-Lee. El WWW usa el protocolo de transferencia de hipertexto (HTTP) y encadena hipertextos muy fácilmente, cambiando así la ruta o camino de la información, la cual entonces puede ser organizada, presentada y accedida en la Internet.

En 1993 - La troncal de la red NSFNET es elevada a "T3" lo que lo habilita para trasmitir datos a una velocidad de 45 millones de bits por segundo, o sea cerca de 1400 paginas de texto por segundo.

En 1993-1994 - El visualizador (browsers) gráfico de web Mosaic y Netscape Navigator aparecen y rápidamente son difundidos por la comunidad de la Internet. Debido a su naturaleza intuitiva y a la interfaz gráfica, estos browsers hacen que los WWW y la Internet sean más atractivos al público en general.

En 1995 - La troncal de la red NSFNET es reemplazado por una nueva arquitectura de redes, llamada vBNS (very high speed backbone network system), esto significa sistema de redes con troncal de alta velocidad, que utiliza los Network Service Providers, (Proveedores de Servicios de Redes), redes regionales y Network Access Points (NAPs o Puntos de Acceso a ala Red correspondiendo su traducción al español)

1.4.- CONCEPTOS FUNDAMENTALES SOBRE REDES.

Para poder concatenar los antecedentes anteriores, es menester conceptuar diversas acepciones técnicas así tenemos que son redes informáticas la manera de conectar varias computadoras entre sí, compartiendo sus recursos e información y estando conscientes una de otra.

Cuando las PC´s comenzaron a entrar en el área de los negocios, el conectar dos PC´s no traía ventajas, pero esto desapareció cuando se empezó a crear los sistemas operativos y el Software multiusuario.

1. Topología de redes: La topología de una red , es el patrón de interconexión entre nodos y servidor, existe tanto la topología lógica (la forma en que es regulado el flujo de los datos) ,como la topología física (la distribución física del cableado de la red).

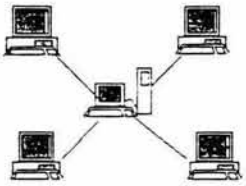
Las topologías físicas de red más comunes son:

a) Estrella.

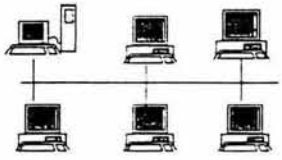
b) Bus lineal

c) Anillo.

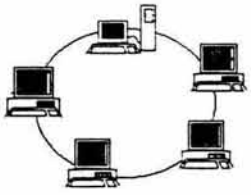
a) Topología de estrella: Red de comunicaciones en que la que todas las terminales están conectadas a un núcleo central, si una de las computadoras no funciona, esto no afecta a las demás, siempre y cuando el "servidor" no esté caído.



b) Topología Bus lineal: Todas las computadoras están conectadas a un cable central, llamado el "bus" o "backbone". Las redes de bus lineal son de las más fáciles de instalar y son relativamente baratas.



c) Topología de anillo: Todas las computadoras están conectados el uno con el otro, formando una cadena o círculo cerrado.



Pero esta interacción de comunicación, no es solamente usando las topologías mostradas, entre ellas existe lo que en técnica informática se llaman Protocolos de intercambio[10], que en informática, como en las relaciones humanas, es la señal mediante la cual se reconoce que puede tener lugar la comunicación o la transferencia de información. Los protocolos de intercambio se pueden controlar tanto con hardware como con software.

Un protocolo de intercambio de hardware, como el existente entre un ordenador o computadora con una impresora o con un módem, es un intercambio de señales, a través de cables específicos, en el que cada dispositivo señala su disposición para enviar o recibir datos.

Un protocolo de software, normalmente el que se intercambia durante las comunicaciones del tipo módem a módem, consiste en una determinada información transmitida entre los dispositivos de envío y de recepción. Un protocolo de intercambio de software establece un acuerdo entre los dispositivos sobre los protocolos que ambos utilizarán al comunicarse. Un protocolo de intercambio de hardware es por tanto similar a dos personas que físicamente estrechan sus manos, mientras que un protocolo de intercambio de software es más parecido a dos grupos que deciden conversar en un lenguaje particular. Pudiendo clasificarse dichos protocolos de la siguiente manera:

a) TCP/IP: (Transmission Control Protocol/Internet Protocol) Protocolo de control de transmisiones/protocolo Internet. Conjunto de protocolos de comunicaciones desarrollado por la Defense Advanced Research Projects Agency (DARPA - Agencia de proyectos de investigación avanzada de defensa) para intercomunicar sistemas diferentes. Se ejecuta en un gran número de computadoras VAX y basadas en UNIX, y es utilizado por muchos fabricantes

[10] Protocolo es la forma de intercomunicación para que entre varios equipos, se reconozcan entre si. http://microasist.com.mx/noticias/tp

de hardware, desde los de computadoras personales hasta los de macrocomputadoras. Es empleado por numerosas corporaciones y por casi todas las universidades y organizaciones federales de los Estados Unidos. El File Transfer Protocol (FTP - Protocolo detransferencia de archivos) y el Simple Mail Transfer Protocol (SMTP -Protocolo simple de transferencia de correspondencia) brindan capacidades de transferencia de archivos y de correo electrónico. El protocolo TELNET proporciona una capacidad de emulación de terminal que permite al usuario interactuar con cualquier otro tipo de computadora de la red. El protocolo TCP controla la transferencia de los datos, y el IP brinda el mecanismo para encaminarla.

b) IPX: (Internet Packet EXchange) intercambio de paquetes entre redes Un protocolo de comunicaciones del NetWare de Novell que se utiliza para encaminar mensajes de un nodo a otro. Los programas de aplicación que manipulan sus propias comunicaciones cliente/servidor o de igual a igual en una red Novell pueden acceder directamente al IPX o al protocolo SPX de NetWare. El IPX no garantiza la entrega del mensaje como lo hace el SPX.

c) NETBEUI: NetBEUI (NETBIOS Extended User Interface) Interfaz de usuario extendido de NetBIOS La realización del protocolo de transporte NetBIOS en LAN Manager y LAN Server. Se comunica con las tarjetas de interfaz de red (NICs) vía NDIS (Network Driver Interface Specification). El término fue originalmente usado para definir el protocolo NetBIOS después que éste fue mejorado para soportar la Token Ring Network.

Una vez definidos las topologías y formas de estructurar una red, es básico el indicar también la clasificación de los tipos de redes, misma que se hace según el lugar y el espacio que ocupen y en base a la tecnología de transmisión.

Si es en base a la tecnología de transmisión tenemos que puede ser por broadcast(canal protagonista) y point to point(punto a punto):

a) Broadcast. Un solo canal de comunicación compartido por todas las máquinas. Un *paquete* mandado por alguna máquina es recibido por todas las otras.

b) Point-to-point. Muchas conexiones entre pares individuales de máquinas, el paquete de información es dirigido a una en especial.

En base al tamaño y espacio que ocupan tenemos la siguiente clasificación

a) LAN - Redes de Área Local.- Es una red que se expande en un área relativamente pequeña. Éstas se encuentran comúnmente dentro de una edificación o un conjunto de edificaciones que estén contiguos. Así mismo, una LAN puede estar conectada con otras LANs a cualquier distancia por medio de línea telefónica y ondas de radio.

Pueden ser desde 2 computadoras, hasta cientos de ellas. Todas se conectan entre sí por varios medios y topología, a la computadora(s) que se encarga de llevar el control de la red es llamada "servidor" y a las computadoras que dependen del servidor, se les llama "nodos" o "estaciones de trabajo".

Las computadoras de una red pueden ser PC´s que cuentan con su propio CPU, disco duro y software y tienen la capacidad de conectarse a la red en un momento dado; o pueden ser PC´s sin CPU o disco duro y son llamadas "terminales tontas", las cuales tienen que estar conectadas a la red para su funcionamiento.

Las LANs son capaces de transmitir datos a velocidades muy rápidas, algunas inclusive más rápido que por línea telefónica; pero las distancias son limitadas.

b) WAN - Redes de Área Amplia.- Es una red comúnmente compuesta por varias LANs interconectadas y se encuentran en una amplia área geográfica. Estas LANs que componen la WAN se encuentran interconectadas por medio de líneas de teléfono, fibra óptica o por enlaces aéreos como satélites.

Entre las WAN mas grandes se encuentran: la ARPANET, que fue creada por la Secretaría de Defensa de los Estados Unidos y se convirtió en lo que es actualmente la WAN mundial: INTERNET, a la cual se conectan actualmente miles de redes universitarias, de gobierno, corporativas y de investigación.

Pero invariablemente, es necesario el uso de herramientas necesarias para armar y construir una red de forma física, llamados tales materiales cómo Componentes de red, y lo que compone una red en forma básica y tangible es lo siguiente:

a) Software.- Podemos conceptuar en un sentido amplio como "una secuencia de instrucciones o indicaciones destinadas a ser utilizadas directa o indirectamente en un sistema informático para realizar una función o tarea o para calcular un resultado cualquiera que sea la forma de su expresión o fijación."

b) Servidor (server).- El servidor es la máquina principal de la red, la que se encarga de administrar los recursos de la red y el flujo de la información. Muchos de los servidores son "dedicados", es decir, están realizando tareas específicas, por ejemplo, un servidor de impresión solo para imprimir; un servidor de comunicaciones, sólo para controlar el flujo de los datos...etc. Para

que una máquina sea un servidor, es necesario que sea una computadora de alto rendimiento en cuanto a velocidad y procesamiento, y gran capacidad en disco duro u otros medios de almacenamiento.

c) Estación de trabajo (Workstation).-Es una computadora que se encuentra conectada físicamente al servidor por medio de algún tipo de cable. Muchas de las veces esta computadora ejecuta su propio sistema operativo y ya dentro, se añade al ambiente de la red.

d) Sistema Operativo de Red.- Es el sistema (Software) que se encarga de administrar y controlar en forma general la red. Para esto tiene que ser un Sistema Operativo Multiusuario, conceptual izándose dicho sistema como aquel en que múltiples usuarios pueden hacer uso de una terminal sin variar o alterar el contenido de la misma, como por ejemplo: Unix, Netware de Novell, Windows NT, etc.

e) Recursos a compartir.- Al hablar de los recursos a compartir, estamos hablando de todos aquellos dispositivos de Hardware que tienen un alto costo y que son de alta tecnología. En éstos casos los más comunes son las impresoras, en sus diferentes tipos: Láser, de color, plotters y todos aquellos perifericos que se necesitan para el desenvolvimiento de dicha red.

f) Hardware de Red.- Son aquellos dispositivos que se utilizan para interconectar a los componentes de la red, serían básicamente las tarjetas de red (NIC-> Network Interface Cards) y el cableado entre servidores y estaciones de trabajo, así como los cables para conectar los periféricos. Teniendo entre ellos:

Routers y bridges: Los servicios en la mayoría de las LAN son muy potentes. La mayoría de las organizaciones no desean encontrarse con núcleos aislados de utilidades informáticas. Por lo general prefieren difundir dichos servicios por una zona más amplia, de manera que los grupos puedan trabajar independientemente de su ubicación. Los routers y los bridges son equipos especiales que permiten conectar dos o más LAN. El bridge es el equipo más elemental y sólo permite conectar varias LAN de un mismo tipo. El router es un elemento más inteligente y posibilita la interconexión de diferentes tipos de redes de ordenadores. Las grandes empresas disponen de redes corporativas de datos basadas en una serie de redes LAN y routers. Desde el punto de vista del usuario, este enfoque proporciona una red físicamente heterogénea con aspecto de un recurso homogéneo.

Brouters: Un disco dispositivo de comunicaciones que realiza funciones de puente (bridge) y de encaminador (router). Como puente, las funciones del "brouter" son al nivel de enlace de datos (estrato 2), independientemente de protocolos más altos, pero como encaminador, administra líneas múltiples y encamina los mensajes como corresponde.

Gateway: pasarela, puerta de acceso Una computadora que conecta dos tipos diferentes de redes de comunicaciones. Realiza la conversión de protocolos de una red a otra. Por ejemplo, una puerta de acceso podría conectar una red LAN de computadoras. Nótese la diferencia con bridge, el cual conecta redes similares.

TRANSMISIÓN DE DATOS EN LAS REDES

La transmisión de datos en las redes, puede ser por dos medios:

a) Terrestres: Son limitados y transmiten la señal por un conductor físico.

b) Aéreos: Son "ilimitados" en cierta forma y transmiten y reciben las señales electromagnéticas por microondas o rayo láser.

1.5.- EL SURGIMIENTO DE LA TECNOLOGÍA P2P, LOS PROGRAMAS ESPÍA O "SPYWARE" Y SU USO POR ALGUNAS EMPRESAS.

El concepto de la tecnología p2p se basa en la tecnología point to point, solo que su variante mas importante surge desde el momento en que se usan servidores dedicados a la transmisión de archivos personales entre las personas que usan ese servidor, pero poniéndolo a disposición de quien en ese momento utilicé ese servidor.

El ejemplo histórico mas claro es el programa napster, que después de su desaparición en 1999, por una resolución judicial estadounidense, obligo al cierre total de este sitio, su servidor y la distribución de el programa, quedando un precedente histórico, social y jurídico de alto realce a nivel mundial.

Las redes P2P convierten el PC del usuario, usado principalmente para recibir información de la Red, en un elemento activo que permite a los navegantes intercambiarse información entre ellos y agrupar capacidad de procesamiento.

Otras aplicaciones mas actuales como freenet o gnutella, permiten el intercambio entre un número ilimitado de usuarios. Al no necesitar de un servidor central son muy difíciles de controlar. Con las que sólo se puede acabar desconectando todos los servidores que hacen que la red funcione.

La lentitud de Gnutella y complejidad de su manejo son dos de sus grandes defectos. Mientras que Napster guarda un inventario constantemente actualizado de los ficheros en los discos de sus usuarios, al utilizar Gnutella hay que ir preguntando servent (en este caso un PC que hace de servidor y de cliente) a servent hasta encontrar lo que se desea.

Con el propósito de evitar la pérdida de eficiencia nacen versiones evolucionadas (Gnutella es un programa escrito en código abierto y por tanto puede ser mejorado de forma constante) como BearShare, LimeWire o ToadNode.

Para hacer funcionar el programa, el usuario debe conocer además la dirección IP y el número de puerto de otra computadora que participe de esta peculiar red. Aunque esto no resulta difícil con la ayuda de Internet, es sin embargo laborioso. De ahí la necesidad de la simplicidad para que su uso se extienda.

Lo mismo sucede con Freenet, todavía en desarrollo. Este programa va un paso más allá, y aunque también necesita de las direcciones IP como fórmula de identificación, cifra y almacena repetidamente los ficheros para dificultar su localización.

Por lo anterior, se puede observar la gran captación económica que se puede lograr, a la par de la información que se puede acceder por el uso de estos programas, en primer grado por el tipo de material que se intercambia; con frecuencia, archivos de sonido, multimedia la cual es el que mezcla audio y video o mas tipos de medios, y en segundo grado, la clase de material que se distribuye con estos programas, que aunque es protegido por los derechos de autor, se distribuye de forma indiscriminada.

Estas observaciones son mínimas, si las comparamos con el hecho de que como individuos, y a la par de la breve explicación que dimos sobre el funcionamiento de las redes, al hacer uso de estos programas, pagamos a parte de los costos para acceder a la Internet, un precio mas alto, la invasión a nuestra intimidad

Para hacerlo, hemos definido que estos programas al instalarse, conllevan una carga que los ha denominado como programas espía o spyware.

Los Spywares o archivos espías diminutas aplicaciones cuyo objetivo es el envío de datos del sistema donde están instalados, mediante la utilización subrepticia de la conexión a la red, a un lugar exterior, el cual por lo general resulta ser una empresa de publicidad de Internet. Estas acciones son llevadas a cabo sin el conocimiento del usuario.

El verdadero nombre de estos archivos espías es ADWARE(O SOFTWARE ADVERTIDOR TRADUCIÉNDOLO), y procede de "Advertissing Supported Software".

Hay que aclarar que, aunque evidentemente tienen cierta similitud con los programas Troyanos[11], los Spyware no representan un peligro de manipulación ajena del sistema, ni de daños a nuestro ordenador por parte de terceros. Sus efectos son, simple y llanamente, la violación de nuestros derechos de confidencialidad de nuestros datos, así como una navegación más lenta.

[11] Aplicaciones que parecen inofensivas, pero que llevan instrucciones maliciosas o destructivas al ordenador que las ejecuta, a fin de dejar desprotegido el equipo para una manipulación externa y sin permiso del usuario. http://microasist.com.mx/noticias/.

Llegan a nuestro sistema de una manera muy sencilla: Los introducimos nosotros mismos, aunque, por supuesto, sin tener conocimiento de este hecho.

Normalmente estos archivos vienen acompañando a programas de tipo "Shareware", gratuito y sobre todo, gratuitos que incorporen publicidad. Estos programas suelen ser una oferta tentadora para multitud de usuarios, ya que algunos de ellos son excelentes programas, útiles y en ocasiones, de los mejores de su categoría. ¿No resulta extraño entonces que su difusión sea gratuita? podría ser, pero la inclusión, en muchos casos, de un banner[12] publicitario que se mantendrá activo mientras dure la utilización del programa parece una correspondencia justa por la utilización gratuita, de tal forma que no levanta sospechas.

Cuando instalamos uno de estos programas, al mismo tiempo introducimos en nuestro sistema los archivos que revelarán nuestros datos a empresas muy interesadas en ellos.

Su funcionamiento se basa Normalmente en estos programas instalan un enlace dinámico de librerías, esto es, un archivo .dll.(DINAMIC LIBRARY LANCE por sus siglas en ingles , archivos necesarios para el funcionamiento de cualquier programa y que traducido seria BIBLIOTECA DINAMICA DE LANZAMIENTO) que se instala automáticamente, en la carpeta System de Windows, cuando instalamos los programas que lo incorporan Este es el caso de los archivos espía tipo Aureate, difundidos por la empresa Radiate.

---

[12] Cuadro publicitario regularmente animado, el cual promociona un producto u servicio. Tomado de un articulo de Jaime Olivera Díaz http://microasist.com.mx/noticias/tp/jodtp2607.shtml.

Los "Aureates" pueden realizar diferentes funciones, dependiendo del archivo concreto. Como ejemplo:

ARCHIVO ADVERT.DLL

Guarda las direcciones de las páginas visitadas en el disco duro, en una carpeta a la que el usuario no tiene acceso. Estos datos son enviados utilizando nuestra conexión a la red, protegidos por encriptación, a los servidores de Aureate usando el puerto 1749 del sistema.

ARCHIVO AMCIS.DLL

Este .dll modifica los claves siguientes del registro[13]:

1.HKEY_CURRENT_CONFIG
2.HKEY_DYN_DATA
3.HKEY_PERFORMANCE_DATA
4.HKEY_USERS
5.HKEY_LOCAL_MACHINE
6.HKEY_CURRENT_USER
7.HKEY_CLASSES_ROOT

Quita el registro del archivo oleaut32.dll de la memoria suministrado por Microsoft y sustituye por sus propias llamadas. Lo registra de nuevo cuando el navegador se cierra. Crea los procesos que se comenzarán siempre que se abra el navegador.

---

[13] Registro es la escritura que realiza un programa para almacenarse en una computadora y realizar la comunicación con el Hardware y el Software que se encuentran dentro del mismo. Tomado de un articulo de Jaime Olivera Díaz
http://microasist.com.mx/noticias/tp/jodtp2607.shtml.

Es interesante conocer que, algunos programas que incorporan este tipo de archivos espías, dejarán de funcionar si estos son eliminados. Pero, por el contrario, si desinstalamos[14] el programa anfitrión, en muchos casos no sucede a la inversa, es decir, el archivo espía permanece quedando totalmente funcional.

El uso que se puede dar a esos datos es en principio, el suponer que esos datos capturados y emitidos son posteriormente comercializados por esta y otras empresas similares, con motivos publicitarios.

Esos datos trasmitidos pueden ser, desde poco relevantes (Número de conexiones, Duración de las mismas, Sistema operativo)pasando por bastante relevantes(Paginas visitadas, Tiempo de estancia en las mismas. Banners sobre los que se pulsa, Descargas de archivos efectuadas) y llegando a ser personalmente relevantes e intimos (Dirección de correo electrónico, Número de dirección IP, DNS de la dirección que efectúa la conexión, es decir, ISP y área del país, Número de teléfono al que se realiza la conexión y contraseña de la misma, si esta última está guardada. Listado de todo el software instalado, extraído del registro)

Tras ver esto, está claro que con esa información se puede establecer un lucrativo comercio, cualquier empresa de publicidad estaría interesada en ellos.

Pero lo cierto es que no se sabe a ciencia cierta el destino de esa información, lo que resulta de por si mucho más preocupante. Algunas empresas

[14] Desinstalar es retirar parte o la totalidad de un programa dentro de una computadora, sea de forma manual o automática, personalizadamente o bajo las caracteristicas que ofrece el fabricante del programa. IBIDEM

denunciadas por emplear este tipo de programas han sido Mattel, utilizando el archivo Broadcast, Real Networks, Netscape navigator entre otros.

Las empresas desarrolladoras de estos Spywares alegan que la identidad del usuario se mantiene siempre a salvo, ya que ningún dato sobre esta es captado, y que si bien recogen información, esta se utiliza "únicamente" con fines de marketing y estadística. Una aseveración ridicula, que podemos ejemplificar de manera burda, si se esgrime este argumento al que se sorprende revisando nuestro buzón de correos sin abrir los sobres.

Pero este tipo de empresas de publicidad disponen de otros recursos además de los archivos espías. Es relevante el caso de la compañía Doubleclick y sus famosas Cookies. Esta empresa las consigue que se descarguen desde páginas que alojen algún banner publicitario de su compañía y las utiliza para rastrear las actividades de los navegantes, en principio, pero el asunto ha suscitado una gran polémica en Estados Unidos, cuando esta empresa decidió asociar la información obtenida de las cookies a una gran base de datos que contenía millones de domicilios americanos. Las autoridades tomaron cartas en el asunto y la empresa dispuso una dirección donde darse de baja de esta utilización por parte de la empresa addoubleclick.

Estas cookies, combinadas con técnicas de archivos espías y Web Bug, como más adelante veremos, establecen una corriente de datos, en ocasiones bastante relevantes como para que nadie quisiera facilitarlos indiscriminadamente, cuya utilización por parte de estas empresas supone para las mismas una actividad lucrativa difícil de eludir por el usuario, el cual se encuentra indefenso, principalmente por desconocimiento del proceso, el cual se realiza "subterráneamente".

WEB BUG.- Un Web Bug es una imagen incrustada en un documento html, esto es, una página web o un mensaje de correo en este formato.

Esta imagen resulta invisible al visitante, ya que su tamaño es inapreciable, pudiendo ser este de un píxel y transparente.

Si la página es descargada, o el correo abierto, el Web Bug puede ser rastreado por la compañía emisora, lo que proporciona información sobre la actividad del usuario en la red.

Las páginas web, y el formato del correo electrónico, que provoca la ejecución del navegador, pueden asimismo introducir en nuestro sistema las conocidas cookies, estos cookies le permitirán al remitente recoger cierta información, como la dirección IP que tenemos en ese momento, el tipo de navegador que usamos, y los datos de las demás cookies almacenadas en nuestro sistema, lo que desvela con exactitud los sitios Web que visitamos.

EFECTOS DE LOS WEB BUGS.

Por ahora tan sólo unas cuantas compañías (Entre ellas Microsoft en conjunción con su afamado programa Windows Media Player) pueden desarrollar esta técnica, aunque esto no quiere decir que únicamente sea esta empresa la que la utilice. Monitorizar nuestros hábitos al navegar de momento no tiene otras connotaciones perjudiciales que no sean la captura de información no autorizada por el usuario, con la violación de la privacidad que ello supone (Al monitorizar mediante un Web Bug la recepción de un mensaje que lo porte, estamos desvelando que dicho mensaje ha llegado a una dirección real, la cual una vez confirmada será blanco seguro de multitud de mensajes no deseados).

Pero esta técnica ya supone una posible futura vía de propagación de virus, tal como apuntan algunos estudios al efecto, ya que el Bug, que requiere una conexión al servidor del remitente, posibilitaría la utilización con fines infecciosos, a la manera de los conocidos troyanos, abriendo una nueva técnica de contagios.

DIALERS O MARCADORES

Se pueden definir como aplicaciones que se auto instalan desde determinadas páginas de contenido llamado pornográfico o aquellas de acceso publico, como los foros de consulta, cuya fuente de financiación es el acceso mediante tarificación especial a través de prefijos 906, Estos programas se introducen por un consentimiento viciado (regularmente se le solicita al usuario que vote por un sitio o dominio Web para su subsistencia o que lo catalogue).

Al introducirse en la maquina, sobre todo en aquellas que su acceso es vía marcador o dial up, marcan un número con el prefijo 906, sin que el usuario lo conozca, y este puede estar navegando directamente en la Web (regularmente de forma mas lenta) o con la inclusión de un sitio pornográfico (que aparece al principio de la sesión de navegación)

Su problema radica en introducirle a la maquina un código malicioso, que aun después de desinstalarse del ordenador afectado, como con el software espía, manda datos sensibles a la compañía que lo diseño, además de no retirarse en la totalidad del mismo.

CAPITULO II

LEGISLACIÓN INTERNACIONAL SOBRE EL DERECHO A LA PRIVACIDAD, DERECHO INFORMÁTICO Y DISPOSICIONES JURÍDICAS NACIONALES APLICABLES.

2.1.- CONVENIOS Y TRATADOS INTERNACIONALES SOBRE DERECHO A LA PRIVACIDAD EN LOS QUE MÉXICO HA SIDO PARTICIPE.

México, por su posición Internacional Neutra, ha tenido ha bien suscribirse a varios cuerpos sobre Derechos Humanos, resaltando la Declaración Universal de Derechos Humanos, la Declaración Americana de los Derechos v Deberes del Hombre mismas que en su cuerpo interpretan lo concerniente al Derecho a la Intimidad, y a no ser perpetrada sin Causa justa, resaltando principalmente la Declaración Universal de Derechos Humanos, la misma en la cuál extraemos el preámbulo y el contenido de los Artículos que refieren directamente , como lo es el Articulo 12 de la Declaración en mención y aquellos que implícitamente relacionan un Derecho a la Intimidad.

Declaración Universal de Derechos Humanos

Preámbulo

Considerando que la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad intrínseca y de los derechos iguales e inalienables de todos los miembros de la familia humana;

Considerando que el desconocimiento y el menosprecio de los derechos humanos han originado actos de barbarie ultrajantes para la conciencia de la humanidad, y que se ha proclamado, como la aspiración más elevada del hombre, el advenimiento de un mundo en que los seres humanos, liberados

del temor y de la miseria, disfruten de la libertad de palabra y de la libertad de creencias.

Considerando esencial que los derechos humanos sean protegidos por un régimen de Derecho, a fin de que el hombre no se vea compelido al supremo recurso de la rebelión contra la tiranía y la opresión;

Considerando también esencial promover el desarrollo de relaciones amistosas entre las naciones;

Considerando que los pueblos de las Naciones Unidas han reafirmado en la Carta su fe en los derechos fundamentales del hombre, en la dignidad y el valor de la persona humana y en la igualdad de derechos de hombres y mujeres, y se han declarado resueltos a promover el progreso social y a elevar el nivel de vida dentro de un concepto más amplio de la libertad;

Considerando que los Estados Miembros se han comprometido a asegurar, en cooperación con la Organización de las Naciones Unidas, el respeto universal y efectivo a los derechos y libertades fundamentales del hombre, y

Considerando que una concepción común de estos derechos y libertades es de la mayor importancia para el pleno cumplimiento de dicho compromiso;

La Asamblea General

Proclama la presente

Declaración Universal de Derechos Humanos como ideal común por el que todos los pueblos y naciones deben esforzarse, a fin de que tanto los individuos como las instituciones, inspirándose constantemente en ella, promuevan, mediante la enseñanza y la educación, el respeto a estos derechos y libertades, y aseguren, por medidas progresivas de carácter nacional e internacional, su reconocimiento y aplicación universales y efectivos, tanto entre los pueblos de los Estados Miembros como entre los de los territorios colocados bajo su jurisdicción.

Artículo 1

Todos los seres humanos nacen libres e iguales en dignidad y derechos y, dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros.

Artículo 2

Toda persona tiene todos los derechos y libertades proclamados en esta Declaración, sin distinción alguna de raza, color, sexo, idioma, religión, opinión política o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición.

Además, no se hará distinción alguna fundada en la condición política, jurídica o internacional del país o territorio de cuya jurisdicción dependa una persona, tanto si se trata de un país independiente, como de un territorio bajo

administración fiduciaria, no autónomo o sometido a cualquier otra limitación de soberanía.

Articulo 3

Todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona.

Artículo 8

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.

Artículo 12

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Artículo 30

Nada en esta Declaración podrá interpretarse en el sentido de que confiere derecho alguno al Estado, a un grupo o a una persona, para emprender y desarrollar actividades o realizar actos tendientes a la supresión de cualquiera de los derechos y libertades proclamados en esta Declaración.

En cuanto a la Declaración de los Derechos y Deberes del hombre tenemos a la intimidad referida dentro del cuerpo de este texto los siguientes artículos:

Declaración Americana de los Derechos v Deberes del Hombre

Art. V.- Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar.

Art. IX.- Toda persona tiene el derecho a la inviolabilidad de su domicilio

Art. X.- Toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia.

Así, los anteriores artículos, invariablemente retoman en su contexto a la Intimidad y privacidad de las personas, como el Bien Jurídico que tutelan implícitamente, y que se ha plasmado en varias legislaciones de varios Estados, como parte incólume y principal de sus Constituciones como mas adelante veremos.

2.2.- DISPOSICIONES RELATIVAS AL DERECHO A LA PRIVACIDAD Y PROTECCIÓN DE DATOS CONTEMPLADAS EN LAS LEGISLACIONES DE OTROS PAÍSES.

La evolución cuantitativa y cualitativa de las investigaciones, conquistas tecnológicas, etcétera, puede tener una incidencia muy profunda en la médula misma del sistema jurídico y, fundamentalmente en el caso de la informática, existe el riesgo cierto de que la inagotable sofisticación conduzca a vulnerar fundamentales derechos de la persona (a la privacidad, igualdad, libertad religiosa). Paralelamente, debemos dejar de lado el misoneísmo, es decir, no tenemos que tener miedo al cambio, al avance, a la evolución. Muy por el contrario, juzgamos conveniente la actualización, la modernización, pero el hecho de cambiar y actualizar no quiere decir de ningún modo que el derecho

deje de proporcionar las respuestas que "debe" dar frente a los potenciales peligros que las modificaciones pudieren entrañar.

Concretamente en el campo de la informática, si bien es cierto que los avances son formidables y que han permitido brindar una serie de soluciones muy importantes, justo es reconocer que esa incesante evolución trae consigo no menos constantes riesgos que merodean en el campo de los derechos fundamentales y frente a los cuales "deben" ser expedidas adecuadas respuestas de corte jurídico-institucional como reaseguro de la sana pervivencia de aquellos.

La sociedad informatizada afronta nuevos riesgos y el derecho "debe" estar a la altura de las circunstancias. Permítasenos una digresión: estamos persuadidos de que no basta con delinear teóricamente un haz de derechos, sino que esos derechos deben estar acompañados necesariamente de herramientas procesales para hacerlos valer, es decir, con aquello que nos va a permitir el acceso a la información.

De nada sirve haber reformado la Constitución nacional, haber incluido una serie de nuevos derechos, haber dotado de jerarquía constitucional a un conjunto de tratados internacionales sobre derechos humanos (con lo cual se amplía el ámbito de derechos y libertades fundamentales del individuo), si no se acompaña tal creación con una política por parte del Estado --nos referimos a una política "jurídica"--, que permita el acceso a la jurisdicción para poder hacer valer esos derechos que tan pomposamente se han elucubrado y declamado a partir de la letra constitucional. De lo contrario, estaríamos ante una nueva muestra de gatopardismo: cambiar todo para que todo continúe igual.

No se trata de plantear la cuestión en términos de una lucha entre la sociedad cibernética y los derechos fundamentales. Juzgamos superada la etapa en que el problema discurría como una tensión dialéctica entre "vida privada vs. computadoras", pues el presente estadio de la evolución de la normativa tuitiva de la información personal constituye una síntesis de los intereses sociales e individuales en juego. Allí se aloja el nudo del problema: en la necesidad de buscar una equitativa conciliación de tales valores. Por una parte, los públicos intereses del Estado de acopiar, de reunir información acerca de las personas que viven en su territorio y, por otro lado, el interés propio de los individuos de buscar protección para sus derechos fundamentales, intentando hacerlos valer en los casos concretos de vulneración de los mismos. En conexión con ello, Sagüés sostiene que el habeas data fue concebido para brindar una respuesta de tipo transaccional entre los intereses de registrantes y de registrados.

La médula del problema que abordamos no estriba en el uso informático; la dificultad aparece cuando dicho uso informático se convierte en abuso informático, momento en que el Estado "debe" hacerse presente, brindando respuestas para tratar de armonizar los intereses en juego y restablecer el equilibrio que se ha roto. Es decir, deparar nuevas respuestas y garantías para los crecientes riesgos que se van planteando. Es que en el contexto de la ineludible obligación del Estado de proporcionar medios jurídicos protectivos a los seres humanos que viven dentro de sus fronteras, no debe quedar fuera la creación de adecuadas garantías para prevenir o repeler los efectos perjudiciales que potencialmente pudieren causarles los fenómenos tecnológicos contemporáneos.

A continuación se abordará un señalamiento sólo enunciativo, obviamente exento de ínfulas de exhaustividad, acerca de las regulaciones establecidas en algunos países europeos y americanos respecto de la protección de datos personales.

A) EN EUROPA

Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y otros instrumentos internacionales y comunitarios.

Adoptado en Estrasburgo (1981) por los Estados miembros del Consejo de Europa, procura (como se expresa en su Preámbulo) "conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos". Cabe recordar que el citado Convenio entró en vigor el 1o. de octubre de 1985.

Su finalidad específica es garantizar --en el territorio de cada Estado parte-- a cualquier persona física, sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales (concretamente, su derecho a la vida privada) frente al tratamiento automatizado de los datos de carácter personal correspondientes a ella.

El campo de aplicación del Convenio se circunscribe a los ficheros y al tratamiento automatizado de datos de carácter personal, en los sectores público y privado.

En el capítulo II, se establecen algunos principios básicos para la protección de datos, fijándose el compromiso de cada Estado parte de tomar, en los respectivos derechos internos, las medidas necesarias para la efectivización de los mismos; sucintamente dichos principios son:

Se establece que los datos de carácter personal que sean objeto de un tratamiento automatizado se obtendrán y tratarán leal y legítimamente; se registrarán para finalidades determinadas y legítimas; serán adecuados,

pertinentes y no excesivos en relación con los objetivos para los que se hayan registrado; serán exactos y, si es necesario, actualizados; se conservarán durante un periodo que no exceda del necesario para el cumplimiento de las finalidades tenidas en mira para su registración.

Se determina que ciertas categorías particulares de datos no podrán tratarse automáticamente, a menos que el derecho interno prevea garantías apropiadas.

Deberán tomarse medidas de seguridad apropiadas para la protección de los datos personales contra la destrucción accidental o no autorizada (o la pérdida accidental), así como contra el acceso, modificación o difusión no autorizados.

Asimismo, se conceden ciertas garantías complementarias para la persona concernida, consistentes en: conocer la existencia de un fichero automatizado de datos de carácter personal y de sus finalidades principales; obtener, en intervalos razonables y sin demoras ni gastos excesivos, la confirmación acerca de la existencia o inexistencia del fichero y la comunicación --en forma inteligible-- de los datos que le incumban; obtener la rectificación o supresión de los datos.

Por su parte, se fija como principio general que no se admitirá excepción alguna a las disposiciones de los artículos 5o., 6o. y 8o. del Convenio, salvo cuando tal excepción prevista legalmente por la normatividad de uno de los Estados partes, constituya una medida necesaria en una sociedad democrática para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado, para la represión de infracciones penales, o bien, para la protección de la persona concernida y de los derechos y libertades de otros individuos (artículo 9o.).

Naturalmente, la normativa internacional no se agota con tal Convenio, pues existen numerosas recomendaciones y directivas, por ejemplo:

Del Consejo de Europa, por ejemplo, la Resolución 22 sobre la protección de la intimidad individual frente a los bancos de datos electrónicos en el sector privado, de 26 de septiembre de 1973; Resolución 15 sobre la utilización de datos personales por la policía, de 17 de septiembre de 1987.

De la Comunidad Europea (hoy Unión Europea),por ejemplo, la Resolución del Parlamento Europeo de 1979 sobre la protección de los derechos de la persona frente al avance de los progresos técnicos en el campo de la informática; la Recomendación de la Comisión de 1981 relativa a la Convención del Consejo de Europa para la protección de las personas con respecto al procesamiento automático de datos personales (relating to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data); la Directriz 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995, sobre la protección de los individuos en relación con el tratamiento de datos personales, entre otros.

De la Asamblea General de las Naciones Unidas, en particular las directrices sobre ficheros de datos personales tratados por ordenador.

De la Organización de Cooperación y Desarrollo Económicos (OCDE). Aludimos a las directrices sobre la protección de la intimidad y los flujos transfronterizos de datos, adoptada por su Consejo de Ministros en forma de recomendación a los Estados miembros, con fecha 23 de septiembre de 1980. Con posterioridad a ello (en 1985), se aprobó una declaración atinente a los flujos transfronterizos de datos no personales.

De la Organización Internacional del Trabajo (OIT). Nos referimos al repertorio de recomendaciones prácticas sobre protección de los datos personales de los trabajadores, adoptado por una Reunión de expertos sobre la protección de la vida privada de los trabajadores (realizada del 1o. al 7 de octubre de 1996 en Ginebra, en cumplimiento de una decisión adoptada por el Consejo de Administración de la OIT en su 264a. Reunión --noviembre de 1995). Naturalmente, y como el mismo repertorio indica (artículo 2o.), no tiene carácter obligatorio (lo que también se desprende del modo potencial en que se utilizan los verbos que se emplean en la redacción de algunos de sus textos) y sólo pretende brindar ciertas orientaciones en la materia. De acuerdo con su artículo 4o., se aplica a los sectores privado y público y al tratamiento manual y automático de todos los datos personales de un trabajador (artículo 4.2). Sintéticamente, establece los siguientes principios generales artículo 5o.: El tratamiento de datos personales de los trabajadores debería efectuarse de manera ecuánime y lícita, y limitarse exclusivamente a asuntos directamente pertinentes para la relación de empleo del trabajador artículo 5.1; II) los datos personales deberían utilizarse únicamente con el fin para el que se recabaron artículo 5.2; III) cuando los datos se exploten con fines distintos de aquéllos para los que se colectaron, el empleador debería asegurarse de que no sean utilizados en forma incompatible con esa finalidad inicial y adoptar las medidas necesarias para evitar toda interpretación errada por su aplicación descontextualizada artículo 5.3; IV) las decisiones relativas a un trabajador no deberían basarse exclusivamente en un tratamiento informático de los datos personales a él referidos artículo 5.5; V) los datos personales obtenidos por medios de vigilancia electrónica no deberían ser los únicos factores de evaluación profesional del trabajador (artículo 5.6); VI) los empleadores deberían evaluar en forma periódica sus métodos de tratamiento de datos para reducir el tipo y volumen de la masa de información personal acopiada, y mejorar el modo de proteger la vida privada de los trabajadores artículo 5.7; VII) los trabajadores y sus representantes deberían ser informados de toda actividad de acopio de datos, de las reglas que los gobiernan y de los derechos que les

asisten, artículo 5.8; VIII) el tratamiento de datos personales no debería conducir a una discriminación ilícita en materia de empleo u ocupación ,artículo 5.10 IX) es irrenunciable el derecho de los trabajadores a la protección de su vida privada (artículo 5.13); etcétera.

B)PORTUGAL

La Constitución portuguesa de 1976 (artículo 35) consagra una restricción al poder del Estado en la utilización de la informática y garantiza expresamente el acceso de los ciudadanos a las informaciones que, respecto de ellos, consten en órganos o entidades estatales o privados, pudiendo exigir la rectificación o actualización de aquéllas (cfr. inc. 1). Prohíbe, además, el acceso de terceros a ficheros con datos personales y su respectiva interconexión, así como también los flujos de datos transfronterizos, salvo en los casos excepcionales previstos por la ley (cfr. inc. 2). Por último, proscribe la utilización de la informática en el tratamiento de datos referentes a convicciones filosóficas o políticas, filiación partidaria o sindical, fe religiosa o vida privada, excepto cuando se trate del procesamiento de datos estadísticos no identificables individualmente.

Fue Portugal el primer país europeo que reconoció constitucionalmente la necesidad de proteger a las personas frente a los riesgos informáticos. No obstante ello, hubo de transcurrir un periodo de quince años, para que aquellas disposiciones fueran desarrolladas legislativamente. En efecto, en abril de 1991 se dictó la Ley núm. 10 sobre "protección de datos personales frente a la informática"; normativa que amplía los parámetros tuitivos de la Constitución; prevé la creación de la autoridad de aplicación (Comisión Nacional de Protección de Datos Personales Informatizados –CNPDPI–, en el capítulo II); determina que ninguna decisión judicial, administrativa o disciplinaria puede tomarse considerando como base exclusiva, el perfil de personalidad del titular del registro (artículo 16); y, en síntesis, reproduce los principios consagrados por el "Convenio para la protección de las personas con respecto al tratamiento

automatizado de datos de carácter personal del Consejo de Europa" (de 1981) adoptado en Estrasburgo, al que aludiéramos supra.

C) ESPAÑA

Los artículos constitucionales 18.4 y 105 apartado `b' diseñan el perímetro protector –genérico– del problema que tratamos, y defieren en una ley –orgánica– su tratamiento pormenorizado. El artículo 18.4 (de la Constitución de 1978) reza: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Por su parte, el 105 apartado `b' dispone: "[La ley regulará] b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas". Para dar cumplimiento a la preceptiva constitucional, se dictó la LEY ORGÁNICA NÚM. 5/1992 (DE 29 DE OCTUBRE) SOBRE "REGULACIÓN DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL" (" BOE" núm. 262, de 31 de octubre de 1992). Tal normativa (conocida como LORTAD) constituye un instrumento para impedir que, a través de la tecnología informática, las personas sean blanco de perjuicios en sus derechos.

Su ámbito de aplicación se circunscribe a aquellos datos de carácter personal (entendidos, según el artículo 3.a, como cualquier información concerniente a personas físicas identificadas o identificables) que figuren en ficheros automatizados de los sectores público y privado; incluye, además, toda modalidad de uso posterior –aun cuando no automatizado–, de datos personales registrados en "soporte físico susceptible de tratamiento automatizado" (cfr. artículo 2.1).

Se excluye del espectro aplicativo de la LORTAD: a los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el

almacenamiento de datos para su publicidad con carácter general (artículo 2.2.a); a los ficheros mantenidos por personas físicas para fines exclusivamente personales (artículo 2.2.b); a los de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales (artículo 2.2.c); a los de informática jurídica a los que el público tenga acceso, siempre que aquellos se limiten a reproducir disposiciones o resoluciones judiciales ya publicadas en periódicos o repertorios oficiales (artículo 2.2.d); y a los mantenidos por los partidos políticos, sindicatos e iglesias en la medida que tales datos se refieran a sus asociados, miembros o exmiembros (artículo 2.2.e).

Algunos de los principios de la protección de datos de carácter personal que la normativa estableció, disponen que:

Sólo podrán ser recogidos y tratados automatizadamente aquellos datos adecuados, pertinentes y no excesivos con relación al ámbito y finalidades para los que fueron obtenidos (artículo 4.1), no pudiendo ser utilizados para fines distintos de aquellos para los que se recolectaron (artículo 4.2); deberán ser exactos y actualizados, de modo que respondan verazmente a la situación real del afectado (artículo 4.3); serán cancelados cuando hubiesen dejado de ser necesarios o pertinentes para el objetivo en persecución del cual fueron recabados y registrados (artículo 4.5); deberán ser almacenados de forma que permitan al afectado ejercer el derecho de acceso a los datos (artículo 4.6); se proscribe la recolección de datos por medios fraudulentos, desleales o ilícitos (artículo 4.7).

El tratamiento de datos personales requerirá el consentimiento del concernido, salvo alguna disposición legal en contrario (artículo 6.1). Tal consentimiento no será necesario –entre otros casos– cuando los datos se recojan de fuentes accesibles al público o cuando se recolecten para el ejercicio de funciones

propias de las administraciones públicas en el marco de sus competencias (artículo 6.2).

Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento automatizado los datos personales que revelen ideología, religión y creencias (artículo 7.2). Los datos que refieran al origen racial, a la salud y a la vida sexual solamente podrán ser recabados, tratados y cedidos cuando existan razones de interés general dispuestas por ley, o bien, cuando medie el consentimiento expreso del sujeto concernido (artículo 7.3). Quedan, asimismo, proscriptos los ficheros creados con el exclusivo propósito de almacenar datos personales reveladores de la ideología, religión, creencias, origen racial o vida sexual (artículo 7.4).

El responsable del fichero automatizado y quienes participen en cualesquiera de las etapas del proceso de tratamiento de datos personales están obligados al secreto profesional (artículo 10).

La LORTAD ha establecido los siguientes derechos de las personas:

El afectado podrá impugnar los actos administrativos o decisiones privadas que entrañen una valoración de su conducta, cuyo exclusivo fundamento sea un tratamiento automatizado de datos personales que proporcione una definición de sus características o personalidad (artículo 12).

Cualquier persona podrá conocer la existencia de ficheros automatizados de datos de carácter personal, sus finalidades y la identidad del responsable del fichero; debiendo recabar tal información del Registro General de Protección de Datos, el que será de consulta pública y gratuita (artículo 13).

Se acuerda al afectado el derecho de acceso a los ficheros automatizados para solicitar y obtener información de sus datos de carácter personal (artículo 14.1), derecho que podrá ser ejercitado a intervalos no inferiores a doce meses salvo que acredite un interés legítimo, hipótesis en la cual podrá hacerlo dentro de un plazo menor (artículo 14.3). La información podrá consistir en la mera consulta por visualización de los ficheros o en la comunicación de los datos por escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible (artículo 14.2).

También se establece el derecho de rectificación y cancelación, para el supuesto de que los datos personales resulten inexactos o incompletos (artículo 15.2). La cancelación no será procedente cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros, o cuando mediase obligación de conservar los datos (artículo 15.4). No se exigirá contraprestación alguna para la rectificación o cancelación de los datos personales inexactos (artículo 16.2).

Los afectados que, como consecuencia del incumplimiento de la LORTAD por parte del responsable del fichero, sufran daño o lesión en sus bienes o derechos, tendrán derecho a ser indemnizados (artículo 17.3).

Ejemplificativamente, y para concluir este breve repaso, recordamos que la LORTAD fue complementada con posterioridad entre otros instrumentos normativos por los Reales Decretos:

a) Número 428/1993 (26 de marzo), por el que se aprueba el Estatuto de la Agencia de Protección de Datos (que, conforme el artículo 1.1 de dicho Real Decreto, es un ente de derecho público que tiene por objeto la garantía del cumplimiento y aplicación de las previsiones de la LORTAD, actuando con

plena independencia de las administraciones públicas y relacionándose con el gobierno a través del Ministerio de Justicia --artículo 1.2--), y

b) Número 1.332/1994 (20 de junio), por el que se desarrollan determinados aspectos de aquella Ley Orgánica, v. gr. la transferencia internacional de datos (cap. II), la notificación e inscripción de ficheros (cap. III), el procedimiento sancionador (cap. V), etcétera.

D) ALEMANIA

El Tribunal Constitucional (acompañado por la doctrina) ha consagrado el derecho a la autodeterminación informativa, derecho que subyace, también, en la Ley Alemana Federal de Protección de Datos --de 20 de diciembre de 1990--. En el contexto alemán, es importante destacar como antecedente (que deviene trascendente por sus reflejos anticipatorios en el ámbito europeo), a la Ley del Land de Hesse de Protección de datos (de 7 de octubre de 1970, modificada en 1986), que propendía a la defensa del derecho de la personalidad frente a la utilización de datos, limitando su previsión normativa a los archivos y bancos de datos públicos; sin embargo, contrarrestó tal restricción aplicativa, con la creación de un Comisario para la Protección de Datos (Datenschutzbeauftragter) que tenía a su cargo la supervisión del cumplimiento de la ley.

E) FRANCIA

Es importante destacar la Ley número 78-17 de 6 de enero de 1978, denominada "Ley de Informática, Ficheros y Libertades", de la que se ha sostenido que "constituye una referencia en la materia en toda Europa".

Sobresale, por su importancia, la previsión de su artículo 2o., que establece: "Ningún fallo de los Tribunales de Justicia, que implique la apreciación de

comportamientos humanos podrá tener por fundamento un tratamiento automático de información que pretenda dar una definición del perfil de la personalidad del interesado" (párrafo 1o.); precepto que se completa con una proscripción casi idéntica relativa a que ninguna decisión administrativa o privada podrá tener por único fundamento aquel tratamiento automático de información que intente proporcionar una definición del perfil o personalidad del interesado.

Por su parte, el artículo 6o. prevé la creación de la Comisión Nacional de Informática y Libertades (que, por el artículo 8o., es concebida como una "autoridad administrativa independiente"), que tendrá a su cargo velar por el respeto de las disposiciones de la ley que comentamos.

Otros preceptos dignos de mención --ejemplificativamente-- son:

a) Se prohíbe la recolección de datos por cualquier medio fraudulento, ilegal o ilícito (artículo 25).

b) Las personas a las que se refieren las informaciones nominativas deben ser informadas acerca del carácter obligatorio o voluntario de sus respuestas, de las consecuencias de su negativa a informar, de los destinatarios de las informaciones y de la existencia de los derechos de acceso y rectificación (artículo 27).

c) Queda proscrito --salvo autorización expresa del interesado--, grabar o conservar en soportes informáticos datos nominativos que directa o indirectamente se refieran a creencias políticas, filosóficas o religiosas; origen racial o filiación sindical de las personas (artículo 31, párrafo 1o.).

d) Se establece el derecho de toda persona de acceder --demostrando su identidad-- a consultar a los organismos encargados de la ejecución de los tratamientos automatizados, para conocer si los mismos contienen informaciones nominativas y, en tal caso, tomar conocimiento de éstas (artículo 34) --el que deberá vehicularse en formato fácilmente inteligible y corresponder al contenido de lo registrado (artículo 35, párrafo 1o.).

e) El titular del derecho de acceso podrá exigir que las informaciones inexactas, incompletas, equívocas, obsoletas o aquellas cuya recolección, utilización, comunicación o conservación hubiesen sido prohibidas, sean rectificadas, completadas, aclaradas, actualizadas o suprimidas (artículo 36, párrafo 1o.).

F) SUECIA

No sería justo dejar fuera de este breve señalamiento a Suecia, pues la Datalag, de 11 de mayo de 1973, además de haber sido el primer antecedente legislativo nacional en Europa, ha ejercido una enorme influencia en el contexto de tal continente. Cabe recordar que fue objeto de una modificación por Ley de 1 de julio de 1982 (sobre recolección de datos).

Entre sus disposiciones, merecen destacarse: la creación de la Inspección de Datos (para controlar la utilización informática de la información personal); la exigencia de autorización previa para la creación de bancos de datos; la proscripción de procesar juicios valorativos sobre las personas; etcétera. Ya en punto al marco constitucional, corresponde mencionar la inclusión expresa del resguardo a la intimidad personal en relación con el tratamiento de datos personales en el artículo 3o. de la Constitución de dicho país (revisión de 1990).

G) OTROS PAÍSES EUROPEOS

Ejemplificativamente, mencionamos que existen leyes protectivas de los datos personales frente al uso de la informática, en los siguientes países: Austria (Ley 565 de 18 de octubre de 1978); Bélgica (Ley de 8 de diciembre de 1992); Dinamarca (leyes 293 y 294 --ambas de 8 de junio de 1978-- sobre registros privados y registros de la administración pública, respectivamente); Gran Bretaña (Data Protection Act, de 1984); Irlanda (Ley de 1988); Islandia (Ley núm. 63 de 1984); Italia (Ley núm. 121 de 1 de abril de 1981); Luxemburgo (Leyes de 30 de marzo de 1979 y 31 de marzo de 1979); Noruega (Ley 48 de 9 de junio de 1978); los Países Bajos (Ley sobre ficheros de datos personales de 1989); Suiza (Directivas del Consejo Federal sobre el procesamiento de datos por los entes federales, de 16 de marzo de 1981); y, también, Finlandia, etcétera. A nivel constitucional, y además de las reseñadas, mencionamos a la Constitución de los Países Bajos (de 1983, artículo 10), de Hungría (de 1989, artículo 59.1).

H) ESTADOS UNIDOS DE AMÉRICA

Como antecedentes interesantes en ese país, podemos ubicar: La `Privacy Act' de 1974 y la `Freedom of Information Act' (del mismo año), para proteger (y operativizar) el derecho a la intimidad (privacy) y, paralelamente, impedir la manipulación abusiva de las informaciones.

Asimismo, la `Freedom of Information Act' de 1986, que también contiene prescripciones relativas a la revelación de informaciones y a la regulación del derecho de acceso, rectificación o complementación de los registros informáticos.

I) EL DERECHO IBEROAMERICANO

Existen distintas soluciones. Vamos a referirnos a las previsiones constitucionales.

Para cumplir con el objetivo impuesto, hemos fragmentado el presente tema en dos partes:

a) El derecho a la protección de los datos personales (artículo 31 de la Constitución guatemalteca y 15 de la Constitución colombiana), y

b) Concretamente el artículo 5o. LXXII de la Constitución brasileña; artículo 135 de la paraguaya; artículo 200, inciso 3o. de la peruana, y artículo 43, párrafo 3o. de la argentina).

La Constitución guatemalteca, en su artículo 31, dice:

Acceso a archivos y registros estatales: Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales de los partidos políticos.

La Constitución colombiana --del año 1991-- en su artículo 15, primer párrafo, reza:

Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo,

tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

El 2o. párrafo de tal norma dispone: "En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".

De la lectura de ambos textos (guatemalteco y colombiano) podemos entresacar las ideas liminares de lo que es el derecho a la privacidad en cuanto a datos informáticos. Facilita la operativización del derecho del interesado por conocer qué informaciones personales, es decir, qué datos acerca de aquél están contenidos en archivos o bancos de datos públicos o privados. Después de conocida la información no permanece estático, sino que potencialmente puede instrumentar lo que se denomina en doctrina el "derecho de intervención" sobre la información a la que se accedió.

El derecho de acceso estaría dado por la posibilidad de conocer qué información personal consta en el registro o archivo, y el derecho de intervención sería un paso sucesivo que habilita a modificar, actualizar y rectificar esa información accedida.

"a) para asegurar el conocimiento de informaciones relativas a la persona del solicitante, que consten en registros o bancos de datos de entidades gubernamentales o de carácter público" [vemos nuevamente la limitación: se trata de registros o bancos de datos de carácter gubernamental o público, entendiéndose por público el que de modo habitual brinde información -- publicidad-- a terceros; de ello se deduce que la previsión excluye a los registros o bancos de datos privados]; y

b) En el caso de Paraguay, el artículo 135 de su Constitución consagra expresamente la garantía de (en la parte I, título II, capítulo XII), diciendo:

Toda persona podrá acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquéllos, si fuesen erróneos o afectaran ilegítimamente sus derechos.

Entonces, concede la moderna Constitución paraguaya --del año 1992-- el derecho de acceso a la información a los efectos de conocer cuál es el uso o la finalidad para los que se acopian los datos personales del interesado, pudiendo éste solicitar la actualización, rectificación e, inclusive, la destrucción de los mismos.

Una aclaración importante acerca de la normativa constitucional paraguaya: por una parte, no se detiene sólo en la protección atinente a la información acerca de los derechos extrapatrimoniales del individuo, sino que, también, ofrece resguardo a la conectada con sus intereses patrimoniales. Paralelamente, ofrece cobertura a los datos contenidos en los registros oficiales y en los privados (distinguiéndose, en el particular, de la preceptiva del Brasil).

c) En la norma básica del Perú de 1993 (artículo 200, inciso 3o.), puede leerse: "La acción de habeas data procede contra el hecho u omisión por parte de cualquier autoridad, funcionario o persona, que vulnere o amenace los derechos consagrados en el artículo 2o., incisos 5, 6 y 7".

Obviamente, existe una protección más densa pues potencia la acción de habeas data al declararla articulable contra cualquier autoridad, funcionario o persona. Es decir, que no limita la posibilidad de incoar esta "acción de garantía" contra archivos o bancos de datos públicos, sino que también envuelve a los privados. Además, el habeas dataes procedente contra todo hecho u omisión.

J) EN BRASIL

En 1988 la Constitución brasileña, en su artículo 5, numeral LXXII, se refiere al "conocimiento de informaciones relativas a la persona de la impetrante..." y a la rectificación de datos.

Aproximadamente 10 años más tarde, en Brasil se expide la Ley número 9.507, de 12 de noviembre de 1997 que reglamente la disposición constitucional, con base en 23 artículos.

K) EN COLOMBIA

A partir de 1991, el artículo 15 de la Constitución de este país reconoce al habeas data como un derecho fundamental aun no reglamentado.

L) EN PARAGUAY

Es a partir de 1992, teniendo como antecedente los registros obrantes en poder de la Policía Nacional, que la Constitución, en su artículo 135 reconoce el derecho de las personas para acceder a la información que le corresponda en archivos públicos y privados, para conocer la finalidad de esos registros y para actualizar, rectificar o destruir los mismos datos.

M) EN PERÚ

Desde 1993, el artículo 200, inciso 3, de la Constitución establece de manera expresa el habeas data con los objetivos de que el interesado pueda acceder a la información pública, con ciertas limitantes, y evitar la difamación de la persona por la difusión o suministro a terceros de informaciones que afecten la intimidad personal y familiar.

N) EN ECUADOR

El artículo 30 de la Constitución vigente establece el habeas data con los objetos de acceder a los registros, bancos o bases de datos, conocer su uso y finalidad, así como para solicitar la rectificación, actualización, eliminación o anulación de los datos, en caso de que estos sean erróneos o afecten ilegítimamente los derechos de las personas.

La Ley de Control Constitucional de 1997 ya ha reglamentado la acción de habeas data.

O) EN ARGENTINA

La nueva Constitución de 1994, en su artículo 43, en su párrafo tercero, establece el habeas data como un amparo especial.

Sin embargo, pese a la gran demanda porque se regulara en ley secundaria el habeas data, es hasta el año 2000 que se expide la Ley 25326 de Protección de los Datos Personales, publicada en el Boletín Oficial correspondiente al 2 de noviembre del año mencionado.

En Argentina, el habeas data ha tenido gran recepción, y muestra de ello es que las provincias de Buenos Aires (artículo 20, inciso c de la Constitución Local),

Córdoba (artículo 50 de su Constitución), Chubut (artículo 56 de su Ley primaria) y Jujuy (artículo 23, inciso 6, de su Constitución), entre otras, prevén el habeas data.

En México, no obstante la gran tradición y entramado constitucional que se posee, no se ha otorgado a los gobernados la garantía procesal del habeas data. México no puede quedarse atrás de los países europeos y latinoamericanos, máxime si se toma en cuenta que los países que ya regulan el habeas data limitan el movimiento internacional de datos con aquellos países que no brinden condiciones equivalentes de seguridad a las propias, de donde se sigue que México, en alguna medida, se encontraría marginado de este movimiento internacional de datos en diferentes materias en las que pueden incluirse la comercial y económica.

Para contextuar la Ley Argentina en mención, habremos de resumir y retomar solo tres de siete capítulos, estos refieren a la definición jurídica de datos informáticos y su clasificación, asi como la acción que se lleva a cabo y los medios para que el Órgano Jurisdiccional conozca y decida sobre controversias de datos.

Ley 25326 de Protección de los Datos Personales HABEAS DATA publicada en el Boletín Oficial correspondiente al 2 de noviembre del año 2000.

LEY 25.326

Capítulo I

Disposiciones Generales

Disposiciones Generales

Artículo 1° *Objeto*. La presente ley tiene por objeto regular:

a) El uso y tratamiento de datos personales contenidos en archivos, registros, o cualquier otro medio técnico de tratamiento de datos públicos, o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares, y

b) La Tutela jurisdiccional de estos derechos, de conformidad con 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.

Art. 2° *Definiciones*. A los fines de la presente ley se entiende por:

Datos personales. Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

Datos sensibles. Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical o política e información referente a la salud o a la vida sexual.

Archivo, registro, base o banco de datos. Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

Tratamiento de datos. Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Responsable de archivo, registro, base o banco de datos. Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

Datos informatizados. Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

Titular de datos. Toda persona física o de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

Usuario de datos. Toda persona, pública o privada, 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.

Disociación de datos. Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

Medio o redes de difusión pública o semipública de alcance nacional e internacional. Toda utilización de la red Internet, así como sus variaciones Intranet y extranet. Intranet es toda red que utilizando o aprovechando las

tecnologías de Internet se utiliza dentro del ámbito privado. Extranet combina ambos tipos de redes extendiendo su alcance desde el ámbito privado al global siendo soportado por la plataforma existente de Internet.

CAPITULO II

Principios generales relativos a la protección de datos

Art. 3º*Archivo de datos. Licitud*. La formación de archivos de datos será lícita cuando se encuentren debidamente inscritos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia.

Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.

Art. 4º *Calidad de datos.*

1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

4. Los datos deben ser exactos y actualizarse en el caso que ello fuere necesario.

5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados por el responsable del archivo o base de datos, cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.

6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

Art. 5° *Consentimiento.*

1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.

2. No será necesario el consentimiento cuando:

1. Los datos se obtengan de fuentes de acceso público irrestricto;

2. Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

3. Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

4. Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

5. Se trate de datos que tengan fines estadísticos a los que se les hubiera aplicado una operación de disociación;

6. Se trate de información proveniente de operaciones comerciales o financieras que realicen los socios de asociaciones empresarias de informaciones comerciales, sin fines de lucro, con la condición de que esa información se utilice exclusivamente entre los socios de tales asociaciones.

Art. 6° *Información*. Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

1. La finalidad para la que serán tratado y quiénes pueden ser sus destinatarios o clase de destinatarios;

2. La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo de que se trate y la identidad y domicilio de su responsable;

3. El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga en especial en cuanto a los datos referidos en el artículo siguiente;

4. Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;

5. La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Art. 7° *Categoría de datos.*

1. Con la salvedad que se establece en el inciso siguiente, queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles así como también el tratamiento de dichos datos y de cualquiera otro que revele ideología, raza, religión, hábitos personales y comportamiento sexual.

No se considerarán comprendidos, a los fines de la presente ley, en la expresión "hábitos personales" los que se refieran a hábitos de consumo de bienes y servicios, siempre que dichos hábitos no revelen directamente o indirectamente, los comprendidos en la definición de datos sensibles.

2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

3. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

Art. 8º*Datos relativos a las salud.*

Los establecimientos sanitarios públicos o privados y los profesionales vinculados a la ciencia de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional.

Art. 9º *Seguridad de los datos.*

1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

Art. 10.*Deber de confidencialidad.*

1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aún después de finalizada su relación con el titular del archivo de datos.

2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Art. 11. *Cesión.*

1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo. Será nulo el consentimiento cuando no recaiga sobre un cesionario determinado o determinable, o si no constase con claridad la finalidad de la cesión que se consiente.

2. El consentimiento para la cesión es revocable.

3. El consentimiento no es exigido cuando:

1. Así lo disponga una ley;

2. En los supuestos previstos en el artículo 5º apartado 2;

3. Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;

4. Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;

5. Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.

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 semejantes a los que establece la presente ley. En ningún caso podrán ser objeto de transferencia internacional lo datos sensibles.

2. La prohibición no regirá en los siguientes supuestos:

1. Colaboración judicial internacional;

2. Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica en tanto se realice en los términos del inciso e) del artículo anterior;

3. Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicables;

4. Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;

5. Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen;

6. Cuando la transferencia se realice dentro del mismo conjunto económico, entre controlante y controlada o entre sociedades que tengan un controlante común;

7. Cuando el cedente obligue contractualmente al cesionario y se responsabilice frente al titular de los datos, previamente a la transferencia, a cumplir con las normas de la presente ley.

Capítulo III

Derechos de los titulares de datos

Art. 13. *Derecho de información.* Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita.

Art. 14. *Derecho de acceso.*

1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.

2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informes, éste se estimara insuficiente, quedará expedita la acción de conocimiento en los términos previstos en el capítulo VII sección I de la presente ley.

3. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.

4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.

Art. 15. *Contenido de la información.*

1. La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen.

2. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los dato personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.

3. La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen u otro idóneo a tal fin.

Art. 16. *Derecho de rectificación, actualización o supresión.*

1. Toda persona tiene derecho a que sea rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.

2. El responsable o usuario de un banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de haber recibido el reclamo del titular de los datos o advertido el error o falsedad.

3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de

reparación en los términos previstos en el capítulo VII, sección 1, de la presente ley.

4. En el supuesto de cesión o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.

5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.

6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.

7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.

Art. 17. *Excepciones.*

1. Los responsables de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión de datos de carácter personal en función de la protección de la defensa de la Nación, o de la protección de los derechos e intereses de terceros.

2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se

pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.

3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa.

Art. 18. *Comisiones legislativas*. Las comisiones de Defensa Nacional y la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Seguridad Interior e Inteligencia del Congreso de la Nación y la Comisión de Seguridad Interior de la Cámara de Diputados de la Nación, o las que las sustituyan, tendrán acceso a los archivos o bancos de datos referidos en el artículo 22, inciso 2, por razones fundadas y en aquellos aspectos que constituyan materia de competencia de tales comisiones.

Art. 19. *Gratuidad*. La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado.

Art. 20. *Impugnación de valoraciones personales*.

1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado.

2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos.

Capítulo IV

Usuarios y responsables de archivos, registros y bancos de datos

Art. 21. *Registros de archivos de datos. Inscripción.*

1. Todo archivo, registro, base o banco de datos públicos, y privado destinado a proporcionar informes debe inscribirse en el registro que al efecto habilite el organismos de control.

2. El registro de archivos de datos debe comprender como mínimo la siguiente información:

1. Nombre y domicilio del responsable;

2. Características y finalidad del archivo;

3. Naturaleza de los datos personales contenidos en cada archivo;

4. Forma de recolección y actualización de datos;

5. Destino de los datos y personas físicas o de existencia ideal a las que pueden ser trasmitidos;

6. Modo de interrelacionar la información registrada;

7. Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;

8. Tiempo de conservación de los datos;

9. Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro.

El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el capítulo VI de la presente ley.

Art. 22. *Archivos, registros o bancos de datos públicos.*

1. Las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el Boletín oficial de la Nación o diario oficial.

2. Las disposiciones respectivas deben indicar:

1. Características y finalidad del archivo;

2. Personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas;

3. Procedimiento de obtención y actualización de los datos;

4. Estructura básica del archivo, informatizado o no , y la descripción de la naturaleza de los datos personales que contendrán;

5. Las cesiones, transferencias o interconexiones previstas;

6. Órganos responsables del archivo, precisando dependencia jerárquica en su caso;

7. Las oficinas ante las que se pudiesen efectuar las reclamaciones ejercicio de los derechos de acceso, rectificación y supresión.

En las disposiciones que se dicten para la supresión de los registros informatizados se establecerá el destino de los mismos o las medidas que se adopten para su destrucción.

Art. 23. *Supuestos especiales.*

1. Quedarán sujetos al régimen de la presente ley, los dato personales que por haberse almacenado para fines administrativos, deban ser objetos de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia, y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.

2. El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad,

organismos policiales o inteligencia, sin consentimiento de los afectados queda limitado a aquellos supuestos y categorías de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categoría, en función de su grado de fiabilidad.

3. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

Art. 24. *Archivos, registros o bancos de datos privados.* Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21.

Art. 25. *Prestación de servicios informatizados de datos personales:*

1. Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.

2. Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

Art. 26. Prestación de servicios de información crediticia.

1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés. Los datos relacionados con el incumplimiento de obligaciones dinerarias sólo podrán tratarse si concurren los siguientes recaudos:

1. Existencia previa de una deuda cierta, vencida y exigible, que haya resultado impaga;

2. Requerimiento previo de pago a su deudor o a quien corresponda el cumplimiento de la obligación.

3. A solicitud del titular de los datos, al responsable o usuario del banco de datos le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.

4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hacer constar dicho hecho. En los casos de datos originados en concursos o quiebras este

plazo se extenderá a diez años. Tratándose de obligaciones dinerarias de origine no crediticio, su cancelación u otro modo de extinción implicará que dicha información deberá ser eliminada de los archivos que se ceden. Está a cargo de la entidad crediticia la obligación de notificar a los bancos de datos públicos o privados la cancelación o extinción de la deuda por parte del deudor dentro de las 48 horas de producido. Asimismo deberán notificar fehacientemente al deudor acerca del cumplimiento de esta obligación.

5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios. En caso de que la información contenga incumplimientos el usuario del informe o cesionario debe ponerlo en conocimiento del titular de los datos, dentro del plazo de cuarenta y ocho horas de recepcionada.

Art. 27. *Archivos, registros o bancos de datos con fines de publicidad.*

1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios, o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento. Solo se podrá ceder a un tercero esta información en forma total o parcial si cuenta con el consentimiento expreso y previo del titular de datos, pudiendo esta conformidad para cesiones posteriores ser prestada en el momento de la recopilación.

2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.

3. El titular podrá en cualquier momento solicitar el retiro de datos a los que se refiere el presente artículo.

Art. 28. *Archivos, registros o bancos de datos relativos a encuestas.*

1. Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a la ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable.

2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna.

Capítulo V

Control

Art. 29. *Órgano de control.*

1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones:

1. Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;

2. Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley;

3. Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;

4. Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto, podrá solicitar autorización judicial para acceder a locales, equipos o programas de tratamiento de datos a fn de verificar infracciones al cumplimiento de la presente ley;

5. Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas y otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados;

6. Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia;

7. Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley;

8. Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes para obtener la correspondiente inscripción en el registro creado por esta ley.

1. El órgano de control gozará de autarquía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia de la Nación.

2. El órgano de control será dirigido y administrado por un director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia,

El director tendrá dedicación exclusiva en función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones, incapacidad sobreviviente o condena por delito doloso.

El director, así como también el resto del personal, están obligados a guardar secreto de los datos de carácter personal que conozcan en el desarrollo de su función.

La Fiscalía de Investigaciones Administrativas, a través de un fiscal general competente en la materia, podrá ejercer las facultades previstas en el artículo 45 de la ley 24.946 respecto de la observancia de la presente por parte de todos los archivos, registros y bases de datos públicos. Dictaminará en los asuntos de importancia sometidos a consideración del director; en los casos en que se haya denegado el acceso o rectificación de datos invocando las causales del artículo 17 incisos 1 y 2 su intervención será obligatoria.

Art. 30. *Códigos de conducta.*

1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley.

2. Dichos códigos deberán ser inscriptos 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 reglamentarias sobre la materia.

Capítulo VI

Sanciones

Art. 31.*Sanciones administrativas.*

1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000) a cien mil pesos ($ 100.000), clausura o cancelación del archivo, registro o banco de datos.

2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

Art. 32. *Sanciones penales.*

1. Incorpórase como artículo 117 bis del Código Penal, el siguiente:

1º Será reprimido con la pena de prisión de un mes a dos años el que insertare o hiciere insertar a sabiendas datos falsos en un archivo de datos personales.

2º La pena será de seis meses a tres años, al que proporcionare a un tercero a sabiendas información falsa contenida en un archivo de datos personales.

3º La escala penal se aumentará en la mitad del mínimo y del máximo cuando del hecho se derive perjuicio a alguna persona.

4º Cuando el autor o responsable del ilícito sea funcionario o público en ejercicio de sus funciones, se aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble tiempo que el de la condena.

2. Incorpórase como artículo 157 bis del Código Penal el siguiente:

Será reprimido con la pena de prisión de un mes a dos años el que:

1º A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos accediere, de cualquier forma, a un banco de datos personales.

2º Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años.

Capítulo VII

De la tutela judicial

Sección 1

Acciones especiales de hábeas data

Art. 33. *Objeto.* Las normas contenidas en el presente capítulo tienen por finalidad otorgar a la persona legitimada el acceso a una vía procesal

sumarísima y expedita que le permita obtener del órgano judicial competente, en forma inmediata, la protección o, en su caso, el restablecimiento del pleno ejercicio de los derechos a que se refiere la presente ley, haciendo cesar cualquier tipo de amenaza, intromisión o violación de los mismos.

Art. 34. *Acción de conocimiento.* Toda persona de existencia visible o ideal podrá demandar judicialmente una orden para conocer la amplitud, tenor, destino o uso de los datos referidos a ella acumulados en cualquier tipo de registros o bancos de datos de entidades públicas o privadas, incluidos los destinados a proveer informes y prestación de servicios informatizados.

Art. 35. *Acción de Prevención.* Toda persona de existencia visible o ideal tendrá acción para demandar judicialmente la adopción de todas las medidas que resulten necesarias para impedir que se concrete cualquier clase de violación, restricción, limitación o intromisión ilegítima de sus derechos, en el tratamiento de sus datos personales.

Art. 36. *Acción de reparación.* Toda persona de existencia visible o ideal tendrá acción para demandar judicialmente la supresión, rectificación, actualización o confidencialidad de sus datos personales, en caso de error, falsedad, obsolescencia o discriminación, y el restablecimiento en el goce de los derechos reconocidos por esta ley. Las medidas a adoptar podrán incluir las que resulten necesarias para prevenir o impedir violaciones, restricciones o intromisiones ulteriores.

Art. 37. *Acumulación de acciones.* Las acciones descritas en los artículos anteriores, podrán ser interpuestas en forma autónoma, o ser susceptibles de acumulación.

Sección 2

De las acciones de hábeas data en general

Art. 38. *Legitimación activa*. Las acciones previstas en la sección 1 del presente capítulo, podrán ser ejercidas por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en líneas directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.

Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.

Art. 39. *Legitimación pasiva*. Las acciones procederán respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes.

Art. 40. Competencia. Será competente para entender en las acciones previstas en la sección 1 de este capítulo, el Tribunal Civil del domicilio del actor, del demandado o el del lugar de la amenaza, violación o intromisión ilegítima, a elección del actor.

Art. 41. *Procedimiento*. En todos los casos de ejercicio de alguna de las acciones indicadas en el artículo precedente el procedimiento a aplicar será el de mayor celeridad previsto en la jurisdicción correspondiente, de una vía procesal específica y apta para el ejercicio de dichas acciones no será obstáculo para la actuación del Tribunal, que deberá aplicar el procedimiento previsto que más se adecue al caso planteado, con las adaptaciones que resulten necesarias a fin de lograr la finalidad tutelar eficaz y oportuna.

En el ámbito de la jurisdicción nacional, las acciones mencionadas se tramitarán, por el procedimiento sumarísimo establecido en el Código Procesal Civil y Comercial de la Nación.

Art. 42. *Requisitos de procedencia*. Para la procedencia de las acciones previstas en el presente capítulo, el actor sólo deberá acreditar sumariamente:

1. En el supuesto de la acción de prevención, la existencia de amenaza a alguno de los derechos reconocidos por esta ley;

2. En los supuestos de las acciones de conocimiento y reparación, el cumplimiento de los recaudos previstos en el inciso 2 del artículo 14, y en el inciso 3 del artículo 16, respectivamente.

En ningún caso será necesaria la atribución de culpa o dolo. Son innecesarios la protesta o reclamo administrativo previo, o su agotamiento, cuando la acción judicial se plante contra una persona jurídica pública.

Art. 43. *Medidas cautelares*. Durante la sustanciación de las acciones previstas en el presente capítulo, el tribunal, de oficio o a petición de parte, deberá dictar las medidas cautelares, provisionales o de urgencia que resulten necesarias para hacer cesar de inmediato la amenaza, violación o intromisión ilegítima de los derechos previstos en el presente régimen. El tribunal podrá requerir del actor del cumplimiento de la contracautela pertinente, sólo en el supuesto que por su naturaleza, las medidas a adoptar sean susceptibles de causar perjuicio a la parte demandada.

Art. 44. *Sentencia.* La sentencia que haga lugar a la acción ordenará la adopción de las medidas necesarias para asegurar la protección o el restablecimiento del derecho afectado, debiendo en su caso, disponer la rectificación, actualización o eliminación de los datos de carácter personal, sin perjuicio de la indemnización que pudiera corresponder. En caso de deducirse recurso de apelación éste tendrá sólo carácter devolutivo.

Art. 45. *Compatibilidad con otros procesos.* El ejercicio de las acciones de protección y defensa previstas en este capítulo no obstará al trámite de naturaleza penal que pudiera corresponder, ni el reclamo por los daños y perjuicios causados que se ejercerá según lo dispuesto en las normas pertinentes. La existencia de causa penal no será obstáculo para el dictado de sentencia en las acciones previstas por esta ley.

Art. 46. *Presunción.* En los supuestos en que se demande judicialmente el resarcimiento de los daños ocasionados, la existencia de perjuicio se presumirá siempre que se acredite la violación o intromisión ilegítima en los derechos reconocidos por esta ley. La indemnización se extenderá al daño moral que se valorará atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente producida. La condena podrá incluir la difusión y/o publicación de la sentencia por los medios que resulten necesarios para la adecuada compensación del perjuicio causado. La indemnización nunca será inferior a 5.000.

Art. 47. *Ámbito de aplicación.* Las normas de la presente ley contenidas en los capítulos I, II, III, IV y VII, y artículo 32 son de orden público y de aplicación en todo el territorio nacional.

Se invita a las provincias y a la Ciudad Autónoma de Buenos Aires a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional.

La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional.

Art. 48. El Poder Ejecutivo deberá reglamentar la presente ley y establecer el organismo de control dentro de los ciento ochenta días de su promulgación.

Art. 49. *Disposiciones transitorias.* Los archivos, registros, bases o bancos de datos destinados a proporcionar informes existentes al momento de la sanción de la presente ley, deberán inscribirse en el registro que se habilite conforme lo dispuesto en el artículo 21 y adecuarse a lo que dispone el presente régimen dentro del plazo que al efecto establezca la reglamentación.

Art. 50. Comuníquese al Poder Ejecutivo.

2.3.- DISPOSICIONES JURÍDICAS NACIONALES RELACIONADAS CON EL DERECHO A LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS INFORMÁTICOS.

CODIGO PENAL Y PROCEDIMIENTOS PENALES DE SINALOA

Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de delitos, consideramos pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

Título Décimo

"Delitos contra el patrimonio"

Capítulo V

Delito Informático.

Artículo 217.- *Comete delito informático, la persona que dolosamente y sin derecho:*

I.Use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; o

II.Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Al responsable de *delito informático* se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

En el caso particular que nos ocupa cabe señalar que en Sinaloa se ha contemplado al delito informático como uno de los delitos contra el patrimonio, siendo este el bien jurídico tutelado.

Consideramos que se ubicó al *delito informático* bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícitos, pero a su vez, cabe destacar que los *delitos informáticos* van más allá de una simple violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de éstos, no solamente se lesionan esos derechos, sino otros como el derecho a la intimidad.

ALLANAMIENTO DE MORADA

Considerando a esta como la introducción furtiva, mediante engaño violencia y sin autorización de quien deba otorgarla sin causa justificada u orden de autoridad competente a un departamento, vivienda, aposento

1)"La introducción, furtiva, mediante engaño, violencia y sin autorización ..."

2)"Sin causa justificada u orden de autoridad competente..."

3)"A un departamento, vivienda, aposento o dependencia de una casa habitada..."

4)"Realizada directa o indirectamente por una autoridad o servidor público..."

5)"Indirectamente por un particular con anuencia o autorización, de la autoridad."

Fundamentación o Referencia:

Constitución Política de los Estados Unidos Mexicanos

Art. 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.

Código Penal

Art. 285.- Se impondrá de un mes a dos años de prisión y multa de diez a cien pesos al que, sin motivo justificado, sin orden de autoridad competente y fuera de los casos en que la ley lo permite, se introduzca, furtivamente o con engaño

o violencia, o sin permiso de la persona autorizada para darlo, a un departamento, vivienda, aposento o dependencia de una casa habitada.

REVELACIÓN ILEGAL DE INFORMACIÓN RESERVADA

Denota:

1) "La divulgación de información o comunicación reservada, recibida con motivo de un cargo público. . ."

2) "Realizada directa o indirectamente por una autoridad o servidor público..."

3) "Sin fundamentación legal, causando perjuicio a cualquier persona."

Fundamentación o Referencia:

Código Penal

Art. 210.- Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.

VIOLACIÓN A LA CORRESPONDENCIA

Denota:

1) La acción de abrir, destruir, desviar, o sustraer alguna pieza de correspondencia cerrada, confiada al correo.

Fundamentación o Referencia:

Constitución Política de los Estados Unidos Mexicanos

Art. 16. La correspondencia que bajo cubierta circulen por la estafeta estará libre de todo registro, y su violación será penada por la ley...

Ley General de Vías De Comunicación

Art. 576.- Se aplicará de un mes a un año de prisión o multa de cincuenta a mil pesos al que indebidamente abra, destruya o sustraiga alguna pieza de correspondencia cerrada, confiada al correo.

VIOLACIÓN A LA CONFIDENCIALIDAD DE LAS COMUNICACIONES TELEFÓNICAS

Denota:

1) La intromisión ilegal por cualquier medio, en las comunicaciones alámbricas o inalámbricas; telefónicas, telefax o análogas a estas...

2) realizada directa o indirectamente por cualquier autoridad o servidor público o...

3) indirectamente por un particular con la autorización o anuencia de la autoridad o servidor público...

4) en perjuicio de cualquier persona.

5) Las acciones ilegales cuya finalidad sea conocer la identidad de los interlocutores de una comunicación....

6) independientemente de que se de o no a conocer dicha información.

7) La obtención, revelación, divulgación o aprovechamiento de información proveniente de una interferencia.

Fundamentación o Referencia:

Código Penal.

Art. 167.- "Se impondrá de uno a cinco años de prisión y multa de quinientos a cincuenta mil pesos:

"....Al que dolosa e indebidamente intervenga la comunicación telefónica de terceras personas."

CAPITULO III

PROHIBICIÓN DEL USO DE LOS PROGRAMAS ESPÍA O SPYWARE.

3.1.- CONSECUENCIAS JURÍDICAS Y SOCIALES A CORTO, MEDIANO Y LARGO PLAZO DE NO EVITAR LA PROLIFERACIÓN DE ESTOS PROGRAMAS.

La intimidad es un derecho constitucional del individuo (articulo 16 constitucional) que con los medios de comunicación tradicionales, como el correo postal, correo certificado, los apartados de correo, etc., están más que garantizados.

En cambio, con el uso generalizado de los sistemas de comunicación electrónicos, la intimidad y el anonimato de las personas resultan crecientemente amenazados. Cada vez que alguien utiliza el correo electrónico, navega por la Web, interviene en foros de conversación, participa en los grupos de noticias, o hace uso de un servidor, está revelando datos sensibles acerca de su personalidad, economía, gustos, hábitos sociales, residencia, etc., que pueden ser maliciosamente recolectados y utilizados por terceros, en perjuicio del que los usa.

La amenaza más evidente, de la que todo el mundo es consciente, consiste en los ataques a la confidencialidad, autenticidad e integridad del correo electrónico. Hoy día resulta sencillo hacer frente a estos ataques mediante los protocolos de comunicaciones basados en procedimientos criptográficos.

En cambio, la mayoría de los usuarios no es consciente de la cantidad de información privada que, de forma inadvertida e involuntaria, está revelando

a terceros, al hacer uso de la Internet. Cada vez que se visita un sitio Web, se suministra de forma rutinaria una información que puede ser archivada por el administrador del sitio. A éste, no le resulta difícil averiguar la dirección de Internet de la máquina desde la que se está operando, la dirección de correo electrónico del usuario qué páginas lee y cuáles no, qué figuras mira, cuántas páginas ha visitado, cuál fue el sitio recientemente visitado y también qué sistema operativo y qué navegador usa.

Con ello se expone a ser víctima de las últimas plagas que han entrado en la escena de las comunicaciones electrónicas: el correo basura (junk-mail o spam), que puede atiborrar nuestro buzón de correo, empleado por marcas comerciales sin escrúpulos o por aficionados para promocionar indiscriminadamente sus productos por toda la red; la suplantación del usuario, para enviar mensajes ofensivos en su nombre a terceros, que le pueden poner en una situación incómoda; el marketing personalizado, que explota información que los usuarios van revelando inadvertidamente a medida que navega por la Red sobre sus gustos y preferencias, etc.

Pero estos efectos son menores, si los comparamos con el riesgo al ser monitoreados nuestras actividades y ver nuestros datos, sean privados, íntimos o sensibles, del uso inmediato que se les de, pongamos a manera de ejemplo, algunos acontecimientos que se han suscitado últimamente:

Se ha encaminado actualmente el llamado E-gobierno mexicano, que es una manera simplificativa de poder realizar tramites de manera rápida, "segura y fiable en la fuente" además de ser "una innovación continua en la entrega de servicios, la participación de los ciudadanos y la forma de gobernar mediante la transformación de las relaciones externas e internas a través de la tecnología, Internet y los medios de comunicación".

Por lo que algunas Secretarias y Organismos dependientes del Ejecutivo han empezado su adherencia a tal plan, empezando por IMSS, ISSSTE, INFONAVIT y actualmente la Secretaria de Hacienda, al implementar el pago de Impuestos vía Internet, el sello digital "infalsificable" y el uso de la firma electrónica como de validez legal en las transacciones realizadas por Internet.

Todo esto enmarca un futuro prometedor en el desarrollo de la tecnología, la inclusión de nuestro Estado Mexicano con la modernidad tecnológica mundial, pero solo en una mínima sino es que menospreciable parte, por lo que hemos de analizar porque:

A) Si bien es cierto el esquema que se nos presenta es de eficiencia y rapidez, además de un ahorro de recursos humanos que conlleva la realización de dichos tramites, no existe lamentablemente confianza en nuestro Gobierno de que tenga la Infraestructura necesaria para realizarlo, refiriéndonos a tal Infraestructura como el equipo para sostenerlo, basta ver a manera de ejemplo el tramite la Tarjeta Tributaria y el pago de los impuestos correspondientes a este ejercicio, fue francamente imposible realizarlo, los servidores estaban ocupados, o se declaraba claramente caídos, y aunque la responsabilidad recayó en los bancos que no mantuvieron los servidores de manera optima para dicho tramite, su argumento inmediato fue escudarse en que la Secretaria de Hacienda no proporciono el equipo necesario para tal transacción.

Otro ejemplo mas es el registro de examen al Instituto Politécnico Nacional, que ha sido desde 1999 vía Internet, y aunque esta H. Institución ha hecho lo posible de conllevar la realización de tal tramite, por el grueso de los requirientes a ingresar, bloquean el servidor, o peor aun, cuelgan los datos enviados, dejándolos a la vista de quien quiera realizar el mismo tramite.

B) Actualmente no existe un marco jurídico que delimite aprobatoriamente a favor de un gobernado el que haya realizado tal operación, ni mucho menos de reguardir de falsos tales sellos electrónicos, a manera de ejemplo nuestra H. Universidad Nacional Autónoma de México maneja tal tecnología, impidiendo registrar o guardar el símbolo de nuestra amada casa en un archivo para su posterior lectura, pudiendo solo imprimirlo. Pero en el mercado o con una simple vista a las paginas warez[15] o sitios que contengan aun de manera ínfima el desarrollo de seguridad informática, se ofrecen herramientas que franquean dicho sello.

C) Si tomamos en cuenta que el grueso de nuestra población no tiene computadora en su casa, aunado de que no todos tienen acceso a la Internet, se ven requeridos a ir a sitios públicos, los llamados Cybercafes, que regularmente tienen instalado a manera de hacer mas atractiva la navegación al cliente que usa tales servicios, programas espía, tales como el ejemplificado KAZZA o Morpheus en el capitulo I de esta tesis, haciendo factible el enrutar y espiar el grueso de los datos que se recaben en ese lugar, y si consideramos que es un tramite federal obligatorio, la cantidad de datos recabadas es sumamente amplia considerando el gran auge de estos negocios.

D) El ejecutivo, por conducto de la Oficina de la Presidencia para la innovación Gubernamental, ha implementado el uso del llamado e-gobierno en las dependencias del INFONAVIT[16], si concatenamos lo anterior de una manera amplia, podemos dilucidar que junto a los datos requeridos en esta pagina,

---

[15] Warez es el cognoscitivo directo a referirse a paginas de contenido ilegal o aquellas dedicadas a la difusión y uso de técnicas para franquear la seguridad en un programa o en un sitio de Internet., viene tal denominación de una dimorfismo de la palabra inglesa "war" que significa guerra y "ez" que significa "is" traducido "es " por lo que un acercamiento mas cercano a nuestro idioma seria "ez guerra o ezto es guerra" la z se usa como símbolo de rebeldía contra el sistema, según declaratoria de los creadores de tales paginas dado que la z es letra universal en la gran mayoría de los países. HERNANDEZ, CLAUDIO, HACKERS 1.0 Los clanes de la Red 2000 ,Argentina 1999,pag 51

[16] Visítese y obsérvese www.micasa.gob.mx

(numero de seguro, RFC, dirección, numero telefónico, lugar de labor, etc.) que la amplitud de datos que se pueden obtener son altamente sensibles.

Bien pudiera pensarse que este pensamiento es un tanto esquizofrénico, pero actualmente, aunque no necesariamente en el campo de la informática y el Derecho Informático, se han visto ejemplos de invasión a nuestra intimidad y nuestros datos, verbigracia, el que se haya recabado el total del padrón electoral mexicano y se haya vendido a un gobierno extranjero, sin saber que uso se les dará a tales datos.

Un argumento que se esgrime en la actualidad es la Seguridad Nacional, o deberíamos inferir la Seguridad de nuestro vecino del norte, Estados Unidos pero estos ataques que se han suscitado actualmente no es mas que la respuesta radical, irracional y destructiva de las acciones que Estados Unidos ha llevado a cabo en perjuicio de varios Pueblos a lo largo de décadas, a lo que sus aliados o aquellos que por su posición geográfica colindan con ese Estado, necesariamente se verán implicados con él .

Pero sin ahondar en tales preceptos, este ataque a la Intimidad de todos nosotros, disminuido por nuestro apático modo de ser y la ignorancia de las consecuencias futuras, es solo el anuncio de un movimiento mas profundo, en el que el Estado delata con el ojo minucioso de quien todo lo sabe, conoce y castiga, no esta lejos de nuestro futuro.

La red Internet es una herramienta de gran utilidad, una fuente poderosa de difusión de recursos, información, datos, ayuda ecológicamente al usar en forma de formularios electrónicos los contenidos de miles de hojas de papel, abarata recursos materiales y humanos, y sobre todo agiliza la funcionalidad de una empresa y su administración, pero como toda novedad también debe

concientizarse sobre los peligros que existen y la necesidad de regular un marco jurídico no esperando tener, como es común en casi todas las sociedades, la generalización del problema para crear una solución "al vapor".

Socialmente es común el llamado ataque por medio de la Internet por gente especializada con diversos objetivos, desde la mera comprobación de un sistema en construcción o la seguridad del mismo, hasta la destrucción parcial del mismo o peor aun, los datos recabados en el mismo, con la finalidad de fomentar económicamente sus actividades.

Aunque ahora existen herramientas adecuadas y poderosas para el cuidado de los datos que se recaban, que veremos en el siguiente punto, no es menester recalcar que el marco jurídico debe ir a la par de la modernidad, sin rezagarse y convirtiéndose en una forma de protección para el pueblo, y no en instrumento de algunos.

3.2.- LA INFRAESTRUCTURA NECESARIA PARA LA DELIMITACIÓN DEL USO DE LOS PROGRAMAS P2P.

Para iniciar el correcto manejo de la Infraestructura, entendida esta como el "conjunto de elementos o servicios que se consideran necesarios para la creación y funcionamiento de una organización cualquiera"[17], tendremos dos opciones, La primera es enumerar los programas espía que existen en Internet y que se distribuyen en la misma, para que en base a ese listado se prohíba el uso en las empresas públicas o privadas y la segunda es la instalación de programas que eviten el funcionamiento de los mismos o acorten su funcionamiento.

---

[17] Summae Jurídica, DICCIONARIO JURÍDICO ELECTRÓNICO VER. 2003-1

La primera opción desgraciadamente es inviable, puesto que al desaparecer una parte de estos programas, en periodos relativamente cortos surgen otros programas con la misma utilidad y objetivo, esto aunado al hecho de que el principal desarrollador de software a nivel mundial fomenta estas prácticas junto con otras empresas, haciendo difícil si no imposible llevar un conteo de los mismos.

La segunda opción es en forma mediata efectiva, pero conlleva el que el desarrollo de estas herramientas que evitarían la filtración de datos debe de evolucionar, sin embargo los individuos que se dedican a franquear la seguridad en redes o en los programas para alterarlos, rápidamente los dejan obsoletos e ineficaces.

Para tal desarrollo hemos de proponer que la infraestructura para desarrollar tales objetivos se debe basar en lo siguiente:

a) Crear y facultar un Órgano desconcentrado dependiente del Ejecutivo, cuyas funciones serian la observancia y determinación por recomendaciones, de cuales programas violentan directamente por su funcionamiento la privacidad de las personas, visto que será en uno de los apartados del presente trabajo.

b) Fomentar el desarrollo de la plataforma libre o el Software libre, esto con el objetivo de que los desarrolladores de programas tengan a bien corregir inmediatamente los problemas que se susciten por violación a la privacidad de los terceros que involuntariamente pudieran realizar, y en el caso de que el objetivo fuera esa violación, al ser de manera libre su desarrollo este se pudiera eliminar de las funciones del programa, esto además es un ahorro de recursos por pagos de licencias a empresas con derecho de patente que hacen difícil a

nuestro gobierno el que solvente sus propios programas para proteger a los gobernados y su administración.

El concepto de Software libre debemos de comprenderlo de una manera mas profunda, para conceptualizarlo tenemos que el``Software Libre" se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. De modo más preciso, se refiere a cuatro libertades de los usuarios del software:

a) La libertad de usar el programa, con cualquier propósito.

b) La libertad de estudiar cómo funciona el programa, y adaptarlo a las necesidades del usuario. El acceso al código fuente es una condición previa para esto.

c) La libertad de distribuir copias, con lo que se puede ayudar a otro individuo.

d) La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie. El acceso al código fuente es un requisito previo para esto.

Un programa es software libre tendrá las características enumeradas y si los usuarios tienen todas estas libertades. Así pues, se deberá tener la libertad de distribuir copias, sea con o sin modificaciones, sea gratis o cobrando una cantidad por la distribución, a cualquiera y a cualquier lugar. El ser libre de hacer esto significa (entre otras cosas) que no se tiene que pedir o pagar permisos.

También deberá tener la libertad de hacer modificaciones y utilizarlas de manera privada en tu trabajo u ocio, sin ni siquiera tener que anunciar que dichas modificaciones existen. Si publican los cambios, no se tiene por qué avisar a nadie en particular, ni de ninguna manera en particular.

La libertad para usar un programa significa la libertad para cualquier persona u organización de usarlo en cualquier tipo de sistema informático, para cualquier clase de trabajo, y sin tener obligación de comunicárselo al desarrollador o a alguna otra entidad específica.

La libertad de distribuir copias debe incluir tanto las formas binarias o ejecutables del programa como su código fuente, sean versiones modificadas o sin modificar (distribuir programas de modo ejecutable es necesario para que los sistemas operativos libres sean fáciles de instalar).

Para que las libertades de hacer modificaciones y de publicar versiones mejoradas tengan sentido, se debe tener acceso al código fuente del programa. Por lo tanto, la posibilidad de acceder al código fuente es una condición necesaria para el software libre.

Para que estas libertades sean reales, deben ser irrevocables mientras no hagan nada incorrecto; si el desarrollador del software tiene el poder de revocar la licencia aunque no le hayas dado motivos, el software no es libre.

Son aceptables, sin embargo, ciertos tipos de reglas sobre la manera de distribuir software libre, mientras no entren en conflicto con las libertades

centrales. Por ejemplo, *copyleft*[18]. Esta regla no entra en conflicto con las libertades centrales, sino que más bien las protege.

Así pues, quizás hayas pagado para obtener copias de software GNU, o tal vez la haya obtenido sin ningún coste. Pero independientemente de cómo haya conseguido sus copia, siempre se tiene la libertad de copiar y modificar el software, e incluso de vender copias.

``Software libre" no significa ``no comercial". Un programa libre debe estar disponible para uso comercial, desarrollo comercial y distribución comercial. El desarrollo comercial del software libre ha dejado de ser inusual; el software comercial libre es muy importante.

Es aceptable que haya reglas acerca de cómo empaquetar una versión modificada, siempre que no bloqueen a consecuencia de ello la libertad de publicar versiones modificadas.

c) Realizar tratados de coordinación con otros Estados, para que estos informen sobre la aparición de otros programas que violen la privacidad de las personas, con el fin de que dependencias gubernamentales que analógicamente se parecieran a este Órgano desconcentrado, reporten su aparición y el modo de frenar dicho desarrollo.

D) Evitar de cualquier forma la instalación de dichos programas en las computadoras de Universidades Públicas y privadas, pues es un hecho comprobado, que el primer lugar en donde los materiales que se obtienen

---

[18] [``izquierdo de copia"] (expresado muy simplemente) es la regla que implica que, cuando se redistribuya el programa, no se pueden agregar restricciones para denegar a otras personas las libertades centrales. Ir a http://www.pwd.com.mx/spanish/glosario.htm

mediante el uso de estos programas(Audio y video regularmente), es en esas Instituciones educativas, a lo que hemos de recordar que no solamente los programas para obtener archivos de Audio y video realizan tal función, habría que desincorporar del Sistema Operativo Windows las funciones del Reproductor de medios o sustituirlas por otras que previo estudio, no tengan el objetivo de irrumpir la privacidad de las personas.

Para el cumplimiento de tales objetivos, es necesario el incluirlos en el Plan Nacional de Desarrollo Informático, que se ha venido llevando desde el año de 1999, con la obviedad de que su funcionamiento debe estar basado en un proyecto incluyente, viable jurídicamente, no es posible que el Estado se autoproteja solamente dejando a sus gobernados la carga de soportar el que sus datos sean mostrados de forma ambivalente, pues solo demostraría o complicidad implícita o un total desconocimiento y desinterés por la ejecución de estos actos.

Las intenciones de incluir a México como parte de este proyecto debe no solo contemplar los intereses de empresarios, ni mucho menos el que ampare solamente a quien en el caso de tener recursos económicos amplios o un conocimiento que se catalogue como secreto, sino a toda la colectividad.

Son nuestros datos los que circulan en la red, si bien es cierto que crece con gran amplitud la necesidad de Interconectarse para el uso de este medio, sea por la realización de un mero tramite, sea para una simple charla con un desconocido, un pariente o un amigo, o para conseguir de forma fortuita material audiovisual que se necesite, este comportamiento también enlaza un control por Órganos Jurídicos con plena capacidad tecnológica y humana para afrentar los retos en el futuro.

En nuestro caso, y como veremos mas adelante, este órgano desconcentrado que denominaremos de ahora en adelante "Coordinación General Para El Desarrollo De La Información Por Internet Y Medios Electrónicos"(CGDIIME), dependiente del Instituto Mexicano de la Propiedad, en el cual hemos de agregar un apartado en el cual se le dotara a dicha Coordinación de autonomía y el que pueda recomendar el desuso de un programa por ser espía, usando los medios de comunicación, alertando vía Internet y sobre todo concientizando a la sociedad sobre los peligros al tener instalados dichos programas espía.

Un ejemplo menor, pero no viable, es el requerirle al Estado para ciertos tramites, servidores y estaciones de trabajo dentro de las Instituciones Públicas, que los usuarios hagan uso de ellos, esto ya existe en cuanto las estaciones de trabajo en el IMSS, SHCP e ISSSTE, pero a manera de servidor que proveyera el servicio de conexión temporal a Internet únicamente para un tramite seria incosteable, y si solo fueran estaciones de trabajo, la necesidad de ampliar tal servicio nos llevaría a un retroceso en dicho proyecto, pues la aglomeración de individuos para realizar un tramite seria igual que si se realizara personalmente en la Institución.

Pero para ahondar en dichas funciones, nos hemos de concretar al Capitulo siguiente para su adecuado desglosamiento.

CAPITULO IV

DELEGACIÓN DE NUEVAS FACULTADES AL INSTITUTO MEXICANO DE LA PROTECCIÓN INDUSTRIAL EN CUANTO AL USO DE LOS PROGRAMAS ESPÍA Y SU MARCO LEGAL

4.1.- NECESIDAD DE FACULTAR AL INSTITUTO MEXICANO DE LA PROPIEDAD INDUSTRIAL PARA QUE CONOZCA, SUPERVISE Y SANCIONE EL USO INDEBIDO DE ESTOS PROGRAMAS Y DE SU INVESTIGACIÓN CUANDO AFECTEN LA PRIVACIDAD DE TERCEROS.

Como se menciono con anterioridad, la CGDIIME dependerá del Instituto Mexicano de la Propiedad Industrial, se le dotara con plena autonomía para que sus funciones de supervisión, observancia y vigilancia sean llevadas con objetividad, pero es menester que dentro de dicho Instituto y su reglamento, se contemple la creación y operación de la CGDIIME, sus funciones y la forma en que operara, sin embargo esta se regirá por las disposiciones de la Ley de Fomento y Protección de la Propiedad Industrial, para esto habremos de analizar un breve estudio que hace viable la operación de la (CGDIIME) a la actual Ley de Fomento y protección de la Propiedad Industrial, esto con el objetivo de obtener las funciones que ahora realiza y que no se contrapongan a esta Ley Federal , mismos que aparecen en el articulo 6 de la Ley de Fomento y protección de la Propiedad Industrial que a la letra dice: El Instituto Mexicano de la Propiedad Industrial, autoridad administrativa en materia de propiedad industrial, es un organismo descentralizado, con personalidad jurídica y patrimonio propio, el cual tendrá las siguientes facultades:

I.- Coordinarse con las unidades administrativas de la Secretaría de Comercio y Fomento Industrial, así como con las diversas instituciones públicas y privadas, nacionales, extranjeras e internacionales, que tengan por objeto el fomento y protección de los derechos de propiedad industrial, la transferencia de tecnología, el estudio y promoción del desarrollo tecnológico, la innovación, la diferenciación de productos, así como proporcionar la información y la cooperación técnica que le sea requerida por las autoridades competentes, conforme a las normas y políticas establecidas al efecto;

Dentro de este apartado podemos reafirmar que esta Institución tiene los medios para poder determinar el uso que se le puede dar a los programas, puesto que si bien están protegidos como obras literarias, también es necesario el exponer el uso que se les debe dar, ya que la "diferenciación de productos", como es citada, implícitamente demarca una cualitivización en cuanto al uso que se les da a los productos, pudiendo incluirse a los programas de computo, además de hablar de las coordinaciones entre unidades administrativas, la SECOFI, así como las Instituciones Públicas y Privadas, nacionales y extranjeras, por lo que da pie a la creación de la CGDIIME, con las características mencionadas anteriormente.

II.- Propiciar la participación del sector industrial en el desarrollo y aplicación de tecnologías que incrementen la calidad, competitividad y productividad del mismo, así como realizar investigaciones sobre el avance y aplicación de la tecnología industrial nacional e internacional y su incidencia en el cumplimiento de tales objetivos, y proponer políticas para fomentar su desarrollo;

Este apartado nos infiere el que la CGDIIME en dado caso de crearse, tendría facultades para realizar investigaciones sobre la aplicación de los programas de cómputo, si estos llegaran a tener instrucciones de mostrar y enviar información privada para poder impedir tal operación.

IV.- Sustanciar los procedimientos de nulidad, caducidad y cancelación de los derechos de propiedad industrial, formular las resoluciones y emitir las declaraciones administrativas correspondientes, conforme lo dispone esta Ley y su reglamento y, en general, resolver las solicitudes que se susciten con motivo de la aplicación de la misma;

En esta fracción, debe determinar el que las declaraciones administrativas que pudiera expedir la CGDIIME serian, como he propuesto y en este Orden de ideas, primero una recomendación expedita, en la cual la empresa o particular que afectara con alguna instrucción en un programa para recabar información se le incitaría por amigable composición a que retirara dicha instrucción, en dado caso de negativa se anunciará por publicación en medios de comunicación que este programa afecta la privacidad de las personas y posteriormente se le ha de obligar si continúa su negativa a publicar de manera inmediata el Código Fuente del programa.

Los cuestionamientos sobre esta forma de coacción se que serán inmediatos, en primer grado se cuestionara la "tibieza" con que estas sanciones o recomendaciones serian aplicadas, pero hemos de razonar en primer lugar que un programador que no tuviera dicha intención de espiar los archivos de terceros, sea por una mala instrucción o un error en la planeación del mismo, muy comunes en las primeras versiones de un programa, se le hará la mención inmediata para que de buena fe en la instrucción de su programa, componga esa instrucción o la retire del mismo, esto con el fin de seguir promoviendo el desarrollo de software en nuestro país y a nivel mundial, con el fin de obtener una armonía entre el derecho y los intereses del capital.

Particularmente no catalogaría de débil o "tibia" el que por medios de comunicación se difundiera el que un programa de computo se le diera la tacha de espía, puesto que el desarrollo de un programa es con el objetivo de que se

difunda, sea para que se venda la copia autorizada del mismo, o para que en su distribución "gratuita" se implante publicidad por parte de patrocinadores, por lo que el menoscabo económico en el que recaería la persona jurídica que haya realizado dicho programa, seria devastador para su desarrollador, por lo que inmediatamente se vería forzado a cambiar la estructura de dicho programa.

Y en el ultimo caso, el cual es la publicación y difusión del Código fuente, la coacción aplicada a este caso provocaría el menoscabo total del desarrollo del programa en si mismo y el detrimento o desaparición de la persona moral que haya desarrollado tal programa, porque el Código fuente es la estructura del programa factible de modificarse o cambiarse, sin ejecutar(ya que ejecutado no es modificable) por lo que al ponerlo a disposición pública, inmediatamente el derecho de autor(que esta a salvo de otra empresa o tercero, que quisiera retomar como suyo ese proyecto) perdería activos económicos a favor de quien lo ostenta, tal es el caso del programa KAZAA, que en un principio y sin que ninguna autoridad determinara si efectivamente era un programa espía, pero que de hecho si realizaba tal función, se inquirió por los llamados "cibernautas"[19] y los medios de comunicación que efectivamente , se enviaban datos privados a servidores especiales de la red Gnutella, a lo que su dueño inmediatamente y como medio de defensa por la calumnia de la que fue parte(según sus propios argumentos) publico el Código fuente de dicho programa en su pagina por tres días, a lo que un grupo de desarrolladores de Software, compilo dicho Código quitándole las instrucciones como programa espía, creando una versión llamada KAZAA- LITE, de libre distribución, sin publicidad y delimitado únicamente a obtener lo que usuario del mismo desea, haciendo de una operación mercadotecnica con el objetivo de que los usuarios continuaran usando el programa KAZAA, en un detrimento para la empresa en si misma. Pero esto solo aplicaría a lo que se refiere al denominado copyright y no a los programas con copy left, que como dijimos, seria en este caso, mas

---

[19] Ir a http://www.pwd.com.mx/spanish/glosario.htm

factible coaccionar al creador de un programa espía por medio de la publicación por medios electrónicos de comunicación que realiza esta función.

XII.- Promover la creación de invenciones de aplicación industrial, apoyar su desarrollo y explotación en la industria y el comercio, e impulsar la transferencia de tecnología mediante:

a) La divulgación de acervos documentales sobre invenciones publicadas en el país o en el extranjero y la asesoría sobre su consulta y aprovechamiento.

b) La elaboración, actualización y difusión de directorios de personas físicas y morales dedicadas a la generación de invenciones y actividades de investigación tecnológica;

c) La realización de concursos, certámenes o exposiciones y el otorgamiento de premios y reconocimientos que estimulen la actividad inventiva y la creatividad en el diseño y la presentación de productos;

d) La asesoría a empresas o a intermediarios financieros para emprender o financiar la construcción de prototipos y para el desarrollo industrial o comercial de determinadas invenciones;

e) La difusión entre las personas, grupos, asociaciones o instituciones de investigación, enseñanza superior o de asistencia técnica, del conocimiento y alcance de las disposiciones de esta Ley, que faciliten sus actividades en la generación de invenciones y en su desarrollo industrial y comercial subsecuente, y

f) La celebración de convenios de cooperación, coordinación y concertación, con los gobiernos de las entidades federativas, así como con instituciones públicas o privadas, nacionales o extranjeras, para promover y fomentar las invenciones y creaciones de aplicación industrial y comercial;

Este punto reafirma lo dicho, solo que al IMPI le ha faltado impulso para realizar tales funciones, como he mencionado, no hay mejor plataforma para desarrollar tales objetivos que la distribución de herramientas y recursos libres, de fácil obtención y que generen interés para su desarrollo en México se ha empezado a implantar algunos de estos tipos de herramientas, pero su difusión es menor, dado que necesitan de mano de obra calificada y conocimiento técnico, pero habría que razonar si esto es cierto, puesto que un estándar establecido a nivel mundial y que la mercadotecnia maneja como el único y el mejor(entiendase a las compañías Intel que desarrolla los procesadores en las computadoras y Microsoft que es la compañía que distribuye el Sistema Operativo Windows), cierra el paso a posibles competidores, intentando postular ideas de desarrollo, es por eso que, bajo el esquema de querer involucrarse como sistema único, la compañía Microsoft dueña de los Derechos del programa WINDOWS, ha tenido a bien el publicar prontamente su Código fuente, pero solo a los gobiernos de los Estados que así lo requieran, en estaciones de trabajo fijas y determinadas por esta compañía y solo con fines de consulta,[20] por lo que podemos determinar que por esas características no seria software libre, que como hemos mencionado es piedra angular para el desarrollo para evitar el desarrollo del Software espía, esto va de la mano con la fracción siguiente:

XIII.- Participar en los programas de otorgamiento de estímulos y apoyos para la protección de la propiedad industrial, tendientes a la generación, desarrollo y

---

[20] Tomado del la revista PC INTELLIGENT, de Laura Samaniego, Editorial Intelligent, año 2 Numero 4, pag 62.

aplicación de tecnología mexicana en la actividad económica, así como para mejorar sus niveles de productividad y competitividad;

México en cuanto lo que se refiere al desarrollo de software a quedado en un rango muy inferior, pues el objetivo mediato de un productor de software que egresa de una Institución educativa Superior, técnica o medio Superior, sea esta privada o pública, es el colocarse en una empresa establecida, sobre plataformas ya enmarcadas, haciendo encuadrar las perspectivas de superación que tenga una persona y frenar el desarrollo de un programador como tal.

La India a manera de ejemplo, es el tercer desarrollador de Software a nivel mundial, usando básicamente herramientas y software libre para el desarrollo de software (de hecho, la plataforma establecida de mas uso en ese país es Linux, que es una herramienta de libre acceso) incluidos desde aquel que se usa en las oficinas hasta lenguajes de bajo nivel con alto rendimiento. Las declaratorias de lo que es el software libre por parte de los creadores del mismo se basan en la libre determinación para modificar, alterar y mejorar un programa conceptualizado como software libre, al contrario del software con *COPYRIGHT* el software libre tiene cláusulas en las que se prohíbe determinar como propietario del mismo a una persona, rendir informes de utilización a una empresa desarrolladora y sobre todo no publicar el Código fuente del mismo, mismas cláusulas que son reconocidas por los usuarios de la misma y que acrecientan el desarrollo del sistema.

XVI.- Promover la cooperación internacional mediante el intercambio de experiencias administrativas y jurídicas con instituciones encargadas del registro y protección legal de la propiedad industrial en otros países, incluyendo entre otras: la capacitación y el entrenamiento profesional de personal, la transferencia de metodologías de trabajo y organización, el intercambio de

publicaciones y la actualización de acervos documentales y bases de datos en materia de propiedad industrial;

Esto es base para que la CGDIIME obtenga fuentes de información directa y medios para el desarrollo de tal Coordinación, a la par de personal necesario para catalogar un programa de espía previa solicitud, y poder coordinarse con otras dependencias públicas o privadas que eviten el desarrollo de tales programas.

XIX.- Participar en la formación de recursos humanos especializados en las diversas disciplinas de la propiedad industrial, a través de la formulación y ejecución de programas y cursos de capacitación, enseñanza y especialización de personal profesional, técnico y auxiliar;

Esto va de la mano con el fomento que se debe realizar con la educación a nivel nacional, pero reiterando el no concretarse a una solo herramienta como el estándar a obedecer, y enmarando claramente un proyecto incluyente con los sectores empresariales y educativos.

XX.- Formular y ejecutar su programa institucional de operación;

En esta fracción, el programa Institucional deberá incluir inmediatamente cómo oficina a la CGDIIME como una parte integrante del IMPI, para su desarrollo, y para la aplicación de las medidas coercitivas serán por conducto del IMPI y para la concretación de la Coordinadora, su operación se basara en primer lugar en definir los programas que están protegidos por el copyright y los que son respetados por la comunidad por el copyleft, así como el fomento directo a este tipo de herramientas.

XXI.- Participar, en coordinación con las unidades competentes de la Secretaría de Comercio y Fomento Industrial, en las negociaciones que correspondan al ámbito de sus atribuciones, y

XXII.- Prestar los demás servicios y realizar las actividades necesarias para el debido cumplimiento de sus facultades conforme a esta Ley y a las demás disposiciones legales aplicables.

Estas dos fracciones, dan pie a la creación de la CGDIIME, pero como menciono. esta se regirá por la Ley de Fomento y protección de la Propiedad Industrial vigente, a la vez que por el reglamento respectivo, mismo que contemplara , como lo veremos mas adelante, las sanciones que expresamos con anterioridad.

4.2.- PROHIBICIÓN DEL USO DE PROGRAMAS ESPÍA EN FORMA TOTAL Y LA DELIMITACIÓN DE UN MARCO LEGAL ADECUADO.

Pero para concretar el uso adecuado de los programas, el fomento creativo a los desarrolladores del software y hardware, así como considerar a Internet una correcta y segura forma de interactuar sin el riesgo de mostrar datos sensibles e íntimos a quienes no deseamos, se debe de prohibir de forma absoluta la creación de dichos programas, esto como lo hemos venido analizando, con formas alternas de coacción, que son medios comprobables contra individuos que en la regularidad de las veces no tienen un domicilio fijo, y que en anonimato desarrollan tales herramientas con el objetivo de comerciar con los mismos.

Para tal objetivo, la prohibición del desarrollo de los programas espía o SPYWARE debe ser tomada en cuenta como un peligro real y propio, no lejano por cuestiones de desconocimiento de uso de la computadora, pues como

vemos, nuestro Estado Mexicano ya ha empezado a incluir el EGobierno como parte integrante para el desarrollo del país, se debe fomentar la educación y advertir sobre los peligros reales que existen al hacer uso de la Internet, por mas que se intente convencer de la seguridad en los sitios y el apoyo tecnológico, este debe ir acompañado de un marco jurídico sustentable que contemple la prohibición genérica de todo software que atente contra la privacidad de las personas, a lo que proponemos que se anexe una fracción mas en el articulo 6 de la Ley de Fomento y protección de la Propiedad Industrial, en la cual en su cuerpo tendrá inscrito:

"FRACCIÓN XXIII.- Mediante la oficina coordinadora correspondiente, indagar y sancionar al desarrollador de programas de computo que tenga como objetivos:

a) Indagar en los datos particulares que se encuentren almacenados en equipos electrónicos de almacenamiento de datos, de los ciudadanos mexicanos, o en los que en su carácter de extranjeros, realicen operaciones en nuestro país, mediante el uso de comunicaciones privadas o en redes públicas electrónicas.

Se entiende para los efectos del inciso anterior:

I) Equipo electrónico de almacenamiento.- Como aquel dispositivo que contenga elementos magnéticos o de cualquier otra índole que sean capaces de contener y almacenar en el interior de los mismos, datos u información.

II) Red.- La conexión directa de varios equipos electrónicos entre si.

III) Red Pública.- Aquella que con base en lo anterior, dependa directamente de una Institución o Secretaria de Estado y exponga información calificada por las leyes de carácter público.

IV) Red Privada.- Aquella que con base a la fracción segunda del presente inciso, intercomunique directa o indirectamente sea con un equipo electrónico público o entre varios equipos electrónicos privados.

b) Sustraer, modificar o consultar los datos privados, íntimos u sensibles, sin el consentimiento expreso, mediante forma escrita y firmada caligráficamente por quien deba otorgarlo.

c) Crear instrucciones dentro de un programa de cómputo, que sin el consentimiento de una persona, o que de mala fe para permitirle el uso del mismo, le pida enviar información sensible u privada del individuo que haga uso del mismo, aun a titulo de hacer uso del programa de forma gratuita.

d) Cambiar la operatividad de un equipo de computo, en el sentido que cada vez que se interconecte en una red, sea privada o pública, divulgue datos íntimos o sensibles a personas que no estén expresamente reconocidas por las leyes, o que con el animo de ofrecer un servicio, den instrucciones de cualquier forma que divulguen datos públicos o privados a quien solo las leyes facultan para hacerlo.

Para los efectos del presente inciso, se entenderá la operatividad como las instrucciones básicas en un equipo electrónico para que realice las funciones de conexión a una red y para que el funcionamiento básico del equipo.

Las sanciones a las que se hará acreedor quien en realice, distribuya, o fabrique programas de computo que tengan los anteriores fines, aparte de las responsabilidades civiles y penales a las que se haga acreedor, serán en el orden mencionado a continuación, las siguientes:

I) Apercibimiento por escrito, para que el que haya realizado el programa, lo modifique , conminándolo a evitar que dicho programa se distribuya con esa instrucción. Si es la primera versión del programa o una posterior en fase de desarrollo, se indicara por escrito el porque el programa en si realiza tal función.

El apercibimiento surtirá efectos al día siguiente de ser recibido por el que desarrollador del programa de computo, mismo que tendrá un termino de diez días para impugnar dicho apercibimiento.

II) Divulgación por los medios de comunicación de que dicho programa efectúa tales instrucciones de divulgación de datos íntimos o sensibles. Para que opere esta sanción es requerimiento indispensable que el haya recibido el apercibimiento muestre su negativa a acatarlo, sea de manera tacita o expresa dentro de lo que establece la fracción primera del presente inciso.

La divulgación por medios de comunicación no le correrán de ninguna manera gastos y costas al apercibido, para lo que el Instituto Mexicano de la Propiedad Industrial se auxiliara de cualquier medio masivo de comunicación para hacer efectiva la presente sanción.

III) De continuar su negativa, la cual se comprobara si sigue distribuyendo el programa de computo que tenga los efectos de la XXIII del articulo 6 de esta Ley, se procederá a que por los medios necesarios para hacer valer esta resolución, publique el código fuente que hace operar dicho programa, sea por

el medio en que el se distribuía el programa, que siempre será el método preferencial, o por conducto del Instituto Mexicano de la Propiedad Industrial, que tomara las medidas necesaria para hacerse del mismo.

Para efectos de esta fracción, se considera Código fuente las instrucciones escritas, en papel o medios electrónicos, que de forma básica hagan funcionar un programa, para dicha calificación de que el Código Fuente pertenece al programa, siempre se hará esta por peritos.

CONCLUSIONES

PRIMERA.- Podemos afirmar que la imponderante necesidad de legislar en materia de Derecho Informático es necesaria e impostergable, puesto que no hablamos únicamente de los llamados Delitos Informáticos, sino de conductas que a falta de una legislación adecuada, a la par del lamentable desconocimiento por algunos juzgadores y legisladores sea por ignorancia, sea por falsas creencias en las que la tecnología debe estar separada del Derecho, han dejado a la mayor parte de los seres humanos que habitamos y hacemos uso de la Internet a merced de los grandes intereses de las compañías transnacionales, además de sus cómplices que disfrazados como empresas distribuidoras de programas "gratuitos" hacen de nuestra información intima un botín económico.

SEGUNDA.-Subrayamos que un programa de inicio y emprendedor cómo es el E-gobierno, debe ser impulsado, con un sentido Jurídico-Legislativo de rigor, puesto que no es del todo completo, ya que falta el consenso de todos los sectores involucrados, dado que la Legislación actual en esta materia es resultado de una emergencia.

TERCERA.- Afirmamos que ahora una correcta plataforma para evitar el desarrollo de programas de computo que atenten contra la Intimidad de las personas es la legislación en materia Industrial, sobre todo en Instituciones que tienen establecida ya una función protectora de los Derechos de marca y patentes de quienes desarrollan sus ideas, dado que tienen la

Infraestructura necesaria para su adecuado desarrollo e investigación, sobre todo que por programas que afecten nuestros datos Íntimos y privados.

CUARTA.-Creemos firmemente que las nuevas formas de coacción contra quienes desarrollan tales programas que atentan contra la privacidad de las personas, serán efectivas en su aplicación, puesto que se ha demostrado con gran tristeza, que los métodos de coacción personal actuales contra quienes desarrollan tales programas de cómputo se quedan rezagados.

QUINTA.- Afirmamos que la aplicación de la tacha contra quien distribuye estos programas de computo con el objetivo de obtener datos genéricos, privados o íntimos, vera mermado su credibilidad, un factor importante en la industria electrónica e informática, mas si la declaratoria viene de autoridad competente para determinar la infracción en contra de quien sin autorización y aprovechando la buena fe de quien hace uso de dicho programa sea para evaluarlo o para hacer uso del mismo(aunque su utilidad queda al albedrío del usuario final) violenta la intimidad y privacidad de los individuos; por lo que el desarrollador del mismo se vera obligado a cambiar la estructura de su programa y así no se vera lesionado el Desarrollo tecnológico, con fines positivos de quien elaboro tal programa.

SEXTA.- Creemos que además de proteger al falible espíritu desarrollador del programador que se vera beneficiado, tanto en forma económica, con el uso de publicidad, como en forma intelectual y profesional, al serle reconocido su trabajo por los usuarios finales del mismo. Le incentivara con esto a mejorar su calidad sin temor a verse coaccionado de manera injusta.

SÉPTIMA.- Consideramos que es necesaria la observación genérico-constructiva para el desarrollo del software libre en todas las plataformas y

esferas sociales, es decir aquel por el que no se paga licencia, se puede modificar y sobre todo, por su origen, no busca una expansión comercial, sino la correcta distribución de la tecnología y el conocimiento en todo el planeta, dado que en la actualidad la pelea por el desarrollo tecnológico ha dejado atrás en perjuicio de los habitantes de México y del planeta Tierra, relegados nuestros mínimos derechos a simples barreras económicas, sacrificadas en nichos en pos de un beneficio que nunca llegara a la mayoría.

OCTAVA.- Creemos firmemente en que la concientización de el uso de la Internet, mediante un programa impulsado por los diferentes sectores de nuestra sociedad, en donde se exponga a la vez de los beneficios, los peligros incólumes que conllevan el hacer uso de esta tecnología, así como una critica constructiva que acerque a la sociedad con los desarrolladores de programas de computo, no buscando solo la comercialización de sus productos, sino la utilidad social y el impacto que tendrá en la sociedad y sobre todo, en nuestro marco jurídico, hará mas aprovechable el uso de la Red de redes.

NOVENA.- Opinamos que en México es indispensable una cultura Informática, en la cual no se enseñe a los educandos la capacitación en los medios de uso de esta tecnología, si no los riesgos que conlleva el utilizarla, esto como parte integral de la educación en nuestro país y mediante programas educativos bien planteados.

DÉCIMA.- Por lo que, afirmamos que la legislación en materia informática debe surgir en nuestro país de forma especializada en una legislación propia, tomando los ejemplos de España, Ecuador y Argentina, que han tenido a bien el expedir Leyes dedicadas única y exclusivamente a la regulación de los actos Jurídicos realizados por este medio.

ONCEAVA.- En sentido positivo, para que podamos retomar la opinión de juristas Internacionales en materia Informática y especialistas en la misma materia, en el cual encaminan el determinar que es necesario darle al correo electrónico el carácter de domicilio, con los correspondientes derechos que conlleva el implantar esta medida(su inviolabilidad principalmente, a la par de las obligaciones que determina) esto como medida primaria para evitar infiltraciones que ataquen la privacidad de las personas.

DOCEAVA.- Lo que nos lleva a concluir con el razonamiento, que es importante no depender en de las imposiciones directas de los llamados "Gigantes tecnológicos", que al querer realizar una hegemonía imperial, protegen sus intereses al inculcar el uso de sus productos como los únicos, existen una infinidad de desarrolladores que ponen una oferta libre de todo tipo de arancel o impuesto, o pago de regalías a su autor, con óptimos resultados, y que a la par se puede modificar, en uso y provecho de quien los utilice, por lo que es necesario instruir a técnicos, académicos y la población en general del uso que se les puede dar a esos recursos.

ANEXO

Al momento de redactar estas líneas, me he dado por enterado de un grave peligro que se acerca prontamente, concretizando el manejo de nuestros datos privados e íntimos por parte de particulares, la aparición por parte de la compañía Microsoft de su producto llamado *passport* mismo que tiene como objetivo el centralizar las operaciones de intercambio de archivos, mensajes, transacciones económicas, correo electrónico, compra de software(y su consecuente activación) y hardware, entre otras operaciones comerciales y personales.

La forma de utilización es sencilla, el usuario da todos sus datos (dirección de correo, dirección física, numero de tarjeta de crédito que es requisito indispensable, dependientes económicos, país de residencia, sistema operativo, tipo de maquina, entre otros) con el objetivo de que la empresa Microsoft le de un numero de identificación, al realizar el usuario una operación vía Internet, el numero de identificación deberá ser introducido por el mismo(*su passport*), a lo cual la empresa donde se realizo la transacción u operación le dará un número de confirmación, que servirá como comprobante para el pago u autentificación de la operación.

Esta nueva forma de operar por parte de Microsoft a la vez que resume una operación de compra, venta u identificación para el uso de los servicios, evitando el llenado común de formularios un tanto exhaustivos una y otra vez por cada operación realizada, es en verdad atemorizante, si bien es cierto que existe una política de privacidad que protege nuestros datos, no hay garantía de que eso sea cierto, ni del uso que se le de a los mismos, mención aparte de que dicha plataforma ha tenido caídas y su seguridad ha

sido franqueada, lo que ha puesto en peligro los datos de quien opera mediante *passport*.

BIBLIOGRAFÍA

1) LÓPEZ AYLLÓN, SERGIO "El Derecho al la Información" México Porrua 1984.

2) LÓPEZ MUÑIZ, MIGUEL "Tratamiento y recuperación de la Información", Madrid CREI- IBI. 1983

3) NORA SIMÓN Y ALAIN, MIN "Informatización de la Sociedad" México F.C.E. 1983

4) SANDERS DONALD "Informática: presente y Futuro" México Mcgraw Hill, 1986

5) TÉLLEZ VALDES, JULIO "La protección Jurídica de los programas de Computación" Trillas Mexico 1985

6) TÉLLEZ VALDES, JULIO "Derecho Informático" Mcgraw Hill, 1995

7) AZPICUETA HERMILIO TOMAS "Derecho Informático" Abeledo Perrot Buenos Aires 1997

8) BELGRANO ZABALE "El Derecho en la Era Digital", Derecho Informático de fin de siglo" Juris, Argentina 1997

9) BINI RAFAEL "El Internet" Sagitario, España ,1997

10) C. MEJAN MANUEL "El Derecho a la Intimidad" Edit Porrua México 1996

11) BARRAGÁN JULIA "Informática y Decisión Jurídica" Edit Porrua Méx. 1996.

12) BATLLE SALES, GEORGINA"El Derecho A La Intimidad Privada Y Su Regulación" Edit Alcoy, España Marfil, 1972

13) ZAVALA DE GONZÁLEZ, MATILDE M, "Derecho A La Intimidad: Análisis Del Articulo 1071 Bis Del Código Civil A La Luz De La Doctrina, De La Legislación Comparada Y De La Jurisprudencia" Buenos aires : Edit Abeledo-perrot, 1982

14) LUZ CLARA, BIBIANA Manual De Derecho Informático Argentina, Buenos Aires, Edit..Jurídica Nova Tesis, 2001.

15) DAVARA RODRÍGUEZ, MIGUEL ANGEL Derecho Informático Pamplona, España Edit..Aranzadi, 1993.

16) DAVARA RODRÍGUEZ, MIGUEL ANGEL MANUAL DEL DERECHO INFORMÁTICO Pamplona, España : Edit... Aranzadi, 1997.

17) LEÓN SOYLA, EL ARRENDAMIENTO FINANCIERO (LEASING) EN EL DERECHO MEXICANO, México UNAM 1989.

BIBLIOGRAFÍA LEGAL

- Constitución Política de los Estados Unidos Mexicanos.

- Ley General de Vías de Comunicación.

- Ley federal de la Propiedad Industrial.

- Código Penal Federal

- Ley Federal del Derecho de Autor.

- Código de Comercio

- TLC Sexta Parte Capitulo XVII.

OTRAS FUENTES

Revista PC INTELLIGENT, Editorial Intelligent, año 2 Numero 4

http://microasist.com.mx/