UNIVERSIDAD NACIONAL AUTONOMA
DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN

LICENCIATURA EN DERECHO

TRABAJO POR ESCRITO QUE

PRESENTA:

SUÁREZ LARIOS DIANA

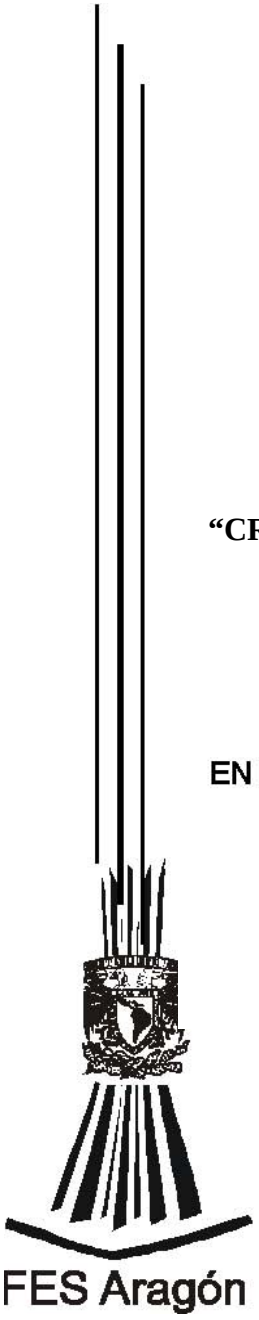
TEMA DEL TRABAJO:

"CRÍTICA A LA PROTECCIÓN JURÍDICA DE LAS BASES DE DATOS PERSONALES EN INTERNET"

EN LA MODALIDAD DE "SEMINARIO DE TITULACIÓN COLECTIVA"

PARA OBTENER EL TÍTULO DE:

LICENCIADO EN DERECHO



MÉXICO 2008

“INDICE”

Pág.

INTRODUCCIÓN

En el presente trabajo se muestra un desarrollo de porque no es efectiva la 1protección jurídica de las bases de datos personales en Internet mediante tres capitulados; en el primero mencionamos de lo que es una base de datos, así como, que es un dato personal, los medios por los cuales se recopilan los mismos y el uso de los mismos. En el segundo capítulo tenemos la legislación que contempla la protección de los mismos partiendo desde el primer nivel jerárquico que es la Constitución hasta las leyes a nivel federal y local. Y por ultimo tenemos el tercer y más importante capítulo que es propiamente la crítica a la creación de variadas leyes pero que se quedan nada más en eso en puras palabras pero nada de acciones.

Actualmente en México la protección jurídica de las bases de datos personales pretende un avance legislativo a raíz de que las mismas bases son conformadas diariamente con mayor rapidez y que en el ámbito de redes informáticas como lo es el caso de INTERNET toma relevancia la regulación y protección de los mismos. Dicha protección de los datos personales es un tema que también en México empieza a ser objeto de debate y discusión, pero desafortunadamente no se cuenta con un marco legal integral que establezca los instrumentos y mecanismos diseñados para tal fin.

La tecnología aplicada a la información en el mundo entero ha tenido una extraordinaria vertiginosidad, prácticamente ha rebasado a la legislación, y todo intento legislativo regula de manera transitoria algunos de los fenómenos informáticos para ser sustituidos por normas novedosas que logran en menor o mayor medida regular la realidad informática.

Sin embargo, en la medida en la que se extienda la penetración y uso de Internet, se debe evaluar la posibilidad de crear un marco jurídico más amplio y eficiente que proteja los datos y la información proporcionada por los ciudadanos no solo a los sitios *web*, a empresas comerciales en caso de realizar operaciones comerciales, sino sobre todo a los órganos gubernamentales cuyos servicios y trámites se ofrecen también en línea hoy en día.

CAPÍTULO PRIMERO
DE LAS BASES DE DATOS Y DE LOS DATOS PERSONALES

Las bases de datos son un conjunto de datos que se encuentran organizados para su almacenamiento en la memoria de un ordenador o computadora, la finalidad de su diseño es para facilitar su mantenimiento y acceso de una forma estándar. La información es organizada mediante campos y registros, en donde un campo se refiere a un tipo o atributo de información, y un registro, a toda la información sobre un individuo. Los datos pueden aparecer en forma de texto, números, gráficos, sonido o vídeo, normalmente las bases de datos presentan la posibilidad de consultar datos, bien los de un registro o los de una serie de registros que cumplan una condición. Para facilitar la introducción de los datos en la base se suelen utilizar formularios; también se pueden elaborar e imprimir informes sobre los datos almacenados.

1.1. Concepto de las bases de datos personales en internet.

Las bases de datos personales en Internet son un conjunto de documentos digitalizados, que cuentan con una estructura que facilita la búsqueda y recuperación de información a través de diferentes mecanismos y herramientas que nos ofrecen cada una de ellas, así como también son el mejor recurso en la web para que los visitantes de un sitio en internet puedan consultar y/o adicionar información de carácter específico con una velocidad asombrosa, en un gran listado de información. La información se encuentra en una computadora u ordenador en donde el usuario se conecta mediante una conexión telefónica para `poder consultarla, una vez realizada la consulta el usuario se desconecta y no vuelve a tener otra relación hasta que no necesita realizar una nueva consulta, estableciendo nuevamente una conexión. [1]

La información es aquel proceso donde se transmiten datos como elemento referencial acerca de una persona o de un hecho y que puede ser susceptible de transmitirse por un signo o una combinación de signos.

---

[1] Dr. DAVARA RODRIGUEZ, Miguel Ángel. “MANUAL DE DERECHO INFORMATICO”, ED. Aranzadi, España 2004 págs.140-141.

Esta información puede incluir imágenes y archivos, no solo texto, de tal manera que puede llegar a ser muy completa. Puede consultarse un pequeño resumen de un registro determinado y mediante un clic, ver más información, en caso del presente trabajo la información o contenido de la misma es de índole personal. Una característica especial de las bases de datos, y que es necesario conocer e interpretar para poder regular la protección jurídica oportuna, es la de su actualización, es decir, que la base de dato cambie respecto a su contenido cada poco tiempo, con las actualizaciones y el aumento de la información correspondiente; debido a esto, la protección debe ser a la base de datos y no a un contenido determinado, ya que la propia dinámica que caracteriza a la base, impediría que se realizara un análisis detallado de su contenido y ese fuese objeto de la protección en cada momento.

Hay que tener, por tanto, en cuenta la característica de la actualización, ampliación y optimización en cuanto al contenido de una base de datos.

PERSONAS QUE INTERVIENEN EN LAS BASES DE DATOS

En una base de datos intervienen, en principio tres personas, con funciones claramente diferenciadas pero con un interés común en el acceso a la información y en la optimización de la respuesta que la base proporcione a las consultas planteadas. Estas tres personas son: a) el creador o promotor, b) el distribuidor y c) el usuario de la base.

a) El creador de la base de datos: Es aquella persona , física o jurídica, que partiendo de un fondo documental adecuado a la materia sobre la que va a versar la base, la crea, mantiene y actualiza, de acuerdo con unas características determinadas.
b) El distribuidor de la base de datos: Es aquella persona física o jurídica que, disponiendo de la estructura informática y comercial adecuada, ofrece la base en el mercado de la información, con la finalidad de captar a usuarios para la consulta y posibilita a estos el acceso a la información y su utilización final.

c) El usuario de la base de datos: Es aquella persona física o jurídica que, estando interesado en consultar documentación de una base de datos, establece una relación con el distribuidor mediante la cual tiene acceso a la información, en las condiciones y con los medios previamente pactados.[2]

1.2. Concepto de los datos personales.

Los datos personales son toda aquella información de carácter personal, traducida en la identificación particular de cada individuo y que abarca los siguientes puntos:

- Filiación: En sentido jurídico es el vínculo que une al progenitor con el hijo, reconocido por el Derecho.
- Fecha de nacimiento: En especifico será establecido o marcado por un día, mes y año determinado en que una persona es concebida
- Lugar de nacimiento: Es aquel lugar o, sitio donde tiene una persona o individuo su origen o principio.
- Domicilio: Aunque por regla general se considera sinónimo de hogar, el estricto sentido jurídico del término alude al lugar que el Derecho considera como residencia de la persona, que puede ser o no el lugar en el que reside en realidad. Toda persona ha de hallarse ubicada dentro de una jurisdicción para que los derechos y obligaciones tengan así un punto concreto de referencia o atribución, de tal modo que su estatus público y privado quede determinado y se conozca dónde ejercerá sus derechos y le serán exigibles sus obligaciones.
- Estado civil: Es aquella situación tipificada como fundamental en la organización de la comunidad, en la que la persona puede verse inmersa y que repercuten en la capacidad de obrar de la misma. Los principales estados civiles son: la nacionalidad, sobre la cual se determina la ley aplicable y la sumisión de un individuo o súbdito a un determinado Estado; al respecto cabe distinguir entre nacionales, extranjeros y apátridas. En segundo lugar, el matrimonio. La familia

[2] *Ídem, pág.136.*

basada en un matrimonio confiere a sus componentes un *status familiae* que difiere según la posición que cada uno de ellos —padres, hijos— ocupan en la misma y, según los casos, puede originar limitaciones de la capacidad de obrar, derechos, deberes, potestades y cargas.

- Ingresos: Se entienden como el dinero, o cualquier otra ganancia o rendimiento de naturaleza económica, obtenido durante cierto periodo de tiempo. El ingreso puede referirse a un individuo.
- Cuentas bancarias: Se traduce como el depósito que hace un individuo en una entidad financiera y que puede disponer del cuando así lo disponga o lo estime conveniente.

- Número de seguro social: El seguro social se conoce como cualquier tipo de asistencia médica disponible y que es suministrada por un sistema de asistencia pública para gente desfavorecida. Esto incluye los hospitales del gobierno y los centros de salud financiados a través de los impuestos. Además de dichos sistemas administrados por los departamentos de salud, pueden existir programas dirigidos por agencias de la seguridad social para empleados de oficinas o industrias. No obstante, allá donde existen estos programas suelen cubrir sólo a una pequeña parte de la población, hay un pequeño estrato de terratenientes, industriales, funcionarios y profesionales (profesionistas) que hacen uso de la medicina privada y sus hospitales.
- Curp. Identificación de tipo credencial de elector que contiene todos los datos de la persona en particular, y
- Número telefónico, entre otros.

1.3. RECOPILACION DE LOS DATOS PERSONALES

Estos datos, al ser recopilados por diferentes centros de acopio tales como lo son los registros civiles, los parroquiales, los médicos, los académicos, los deportivos, los culturales, los administrativos, los fiscales, los bancarios y los laborales; y no por medios exclusivamente manuales sino por medios automatizados, los cuales provocan gran concentración, sistematización e

inmediata disponibilidad sobre este tipo de información para darle diferentes fines originando a su vez bases de datos.[3]
Serán almacenados los datos personales de forma que permitan el ejercicio del derecho de acceso por parte del afectado, a la vez que se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.[4]

En la década de los años 70 surgen numerosos archivos con información de tipo personal, entendiéndose estos como un conjunto mínimo de datos como los anteriormente mencionados, así como también otro tipo de caracteres aún mas distintivos como lo son la raza, la religión, las inclinaciones políticas, los ingresos, las cuentas bancarias y la historia clínica, entre otros.

1.4 **Uso de los datos personales**

Los datos personales son vulnerables según la aplicación de la que sean objeto la cual puede variar; esta información se llega a usar para fines publicitarios, comerciales, fiscales, policíacos, etc. convirtiéndose así en un instrumento manejable. Estos datos se catalogan en archivos de acuerdo a su contenido, es decir, en archivos públicos que son aquellos que maneja el Estado, los archivos privados que manejan únicamente las empresas privadas, los manuales que se procesan de forma manual, automáticos los procesados en forma automática, archivos sobre personas físicas sean o no residentes de un país determinado o personas morales.

Cabe hacer mención que a nivel de derecho positivo no todos estos archivos están sujetos a regulación jurídica.[5]

Los datos de carácter personal no podrán usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos. Deberán ser exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado. Serán cancelados cuando hayan dejado de ser necesarios o

---

[3] Ver anexo 1
[4] GALINDO, Fernando, "Derecho e Informática", Ed. La Ley-Actualidad, España, 1998, pág.77.
[5] www. nacpec.org/es/links/robo_identidad/index.htm,9-octubre-08, 17:35pm

pertinentes para la finalidad para la cual hubieran sido recabados y registrados. La información, de cualquier tipo, es necesaria para determinar políticas, tanto en el sector público como en el privado. De ahí la utilidad de la captura, almacenamiento y difusión de la información personal en los bancos de datos.

1.5 **Figuras jurídicas que intervienen en la protección de los mismos.**

Son variadas las figuras jurídicas bajo las cuales se ha estudiado e intentado regular la protección de los datos personales. En este sentido, tenemos que figuras como los derechos humanos, personales, patrimoniales, libertades públicas y privadas en el caso de Francia, derecho de la privacidad en países anglosajones, derecho a la intimidad y al honor de las personas en España, o aun las garantías individuales y sociales como el caso de México, todas ellas como eventual protección, han tendido hacia una sujeción apropiada en cuanto a la concentración y destino de los datos de carácter personal. No obstante a nivel nacional es insuficiente la regulación de la información y los datos personales.

En materia de protección de datos es mejor la prevención que la curación: es difícil remediar el campo de la infracción de la intimidad. Ha de tenerse en cuenta, que, dada su ambigüedad, es difícil de catalogar la lesión de la intimidad y la indemnización por los daños sufridos. El problema reside en que son muchos los intereses en conflicto. Para que esto se vea en concreto, a continuación se reseña un breve catalogo de las posibles partes en un conflicto relacionado con intimidad, lo que hará ver la dificultad de establecer un esquema de remedios que no consista, tal y como se ha hecho en la legislación mundial, en atender a las actividades de los informáticos como ha quedado reseñado.

El primer implicado es el sujeto de la información personal relevante, y quienes reclaman por él; también está el que recopila la información, incluyendo a todos los que oculta o representa; esta el infractor que violenta ilegalmente el acceso a la información; están los usuarios o la cadena de usuarios que se aprovechan de la acción del infractor.

En un conflicto meramente privado, en el que las partes son distintas unas de otras, el sujeto puede reclamar contra el que captura los datos, el infractor o el usuario, el que captura los datos puede reclamar contra el infractor o el usuario; el usuario puede reclamar contra el infractor.

En muchos casos el interés público puede hacer que se personen en el conflicto las autoridades del estado; tanto contra el infractor, el capturador de los datos o el usuario.

La puesta en práctica de estas acciones puede depender de materias tan difícilmente precisables o controlables como las intenciones de las partes y el carácter razonable o no de sus acciones.[6]

1.6 **Derechos y excepciones**

Toda regulación jurídica engendra derechos y excepciones, y este tema en particular de los datos personales por su misma singularidad, motiva derechos muy especiales como los siguientes:

- DERECHO DE ACCESO: Es aquel derecho que permite a las personas interesadas conocer las instituciones y el tipo de información que dispongan sobre su persona ya sea el cómo, el cuándo y el para qué. El término “acceso” se utiliza para expresar el permiso que tiene un usuario en relación con discos, archivos, registros y procedimientos de entrada en una red. El acceso puede ser total es decir, para ver y modificar la información también conocido como acceso de lectura y escritura, o parcial, es decir. sólo para verla conocido como acceso de lectura.
- DERECHO DE RECTIFICACIÓN. Este derecho permite solicitar a la persona interesada una respectiva modificación en términos de alteración o ampliación, suspensión o cancelación de los datos que referidos a este, considere como inexactos o irrelevantes o que requieran actualizarse.

[6] GALINDO, Fernando, “Derecho e Informática”, Ed. La ley-actualidad, España 1998, págs.88 y 89

- DERECHO DE USO CONFORME AL FIN: Derecho que consiste en que la persona interesada pueda exigir que su información nominativa sea destinada para los objetivos específicos por los cuales se proporciono.
- DERECHO PARA LA PROHIBICIÓN DE INTERCONEXIÓN DE ARCHIVOS: Establece este derecho que las distintas bases de datos existentes no puedan ser consultadas y/o vinculadas de manera indistinta.

CAPÍTULO SEGUNDO

REGULACIÓN QUE PROTEGE A LAS BASES DE DATOS PERSONALES

La regulación de la privacidad y protección de datos personales ha sido abordada a nivel mundial y en forma muy particular por cada país esto se debe, en gran medida, a los intereses económicos y políticos, además de que responde a las estrategias comerciales particulares de cada lugar. Actualmente, el continente europeo es la zona con mayor regulación en cuanto a protección de datos personales se refiere y al flujo transfronterizo de estos, situación que inhibe en forma considerable sus relaciones comerciales con países como Estados Unidos, Canadá y otras naciones asiáticas.[1]

2.1 Regulación Constitucional.

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos representa el marco jurídico de la privacidad en nuestro país. El primer párrafo de este artículo consagra una de las garantías individuales más importantes que es el derecho que tenemos a no ser molestados en nuestra persona, familia, domicilio, papeles o posesiones, sino en virtud de un mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento y en el penúltimo párrafo de este mismo artículo, se contempla que la correspondencia que bajo cubierta circule por las estafetas, deberá estar libre de todo registro y su violación será penada por la ley.

> "ARTICULO 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.
>
> …La correspondencia que bajo cubierta circule por las estafetas, estará libre de todo registro, y su violación será penada por la ley".

Por desgracia el caso de México aún es incierto, a pesar de que en los

[1] ***www.enterate.unam.mx,***

momentos que se escriben estas líneas existe gran efervescencia nacional por el escandaloso manejo de enormes bases de datos, como la electoral a nivel nacional, la de personas con licencia para conducir en la capital del país y del registro vehicular, solo por mencionar algunas. Ni la Constitución federal, u otros tantos ordenamientos jurídicos, son suficientes para regular de, manera adecuada este delicado problema.

La Constitución es muy escasa en este aspecto toda vez que por un lado nos otorga derechos como es el caso del derecho a la información, pero no señala prohibiciones o sanciones para aquellas personas que realicen fraude, chantaje u otros delitos de carácter informático con bases de datos personales, de hecho ni siquiera tiene contemplado el término de base de datos como tal.

Toda vez que la Constitución esta tan concentrada en cuestiones de legisladores y leyes de otra índole que deja de lado o ni siquiera contempla los medios electrónicos como un medio para delinquir o realizar otro tipo de delitos concernientes a la información personal de los particulares, así que por otro lado podemos deducir que respecto a la materia de informático como tal está completamente atrasada por no decir obsoleta.[2]

2.2. Regulación Penal

La delincuencia informática en México es una realidad, en la cual desafortunadamente no hay todavía estadísticas oficiales y si las llega a haber se modifican o alteran, que nos permitan ver con claridad el tema de cuántos delitos informáticos se cometen con la información obtenida por medio de las bases de datos, y lo peor aun es que en materia penal los delitos informáticos no se tienen contemplados en el código ya sea federal o del distrito federal[3].
Pero aún no se sabe mucho de ¿cuántos casos?, ¿cuántos delincuentes se han identificado?, ¿a cuántos han capturado y procesado? Aún peor: ¿Cuáles delitos ya están tipificados en la Ley?, para que en un momento dado haya que sancionar y a quienes sancionar, y obviamente no se tiene estadísticas porque

[2] www.sre-gob/mx/transparencia/info_relevante/basesdedatos.htm
[3] www.ssp.gob.mx/_c_programas/p_cibernetica/INDEX.htm

no es algo que requiera de la atención de las autoridades o no es lo suficientemente “alarmante” para hacer algo al respecto y en caso de que medio se pretenda dar solución no se realiza de manera adecuada como lo es darle un seguimiento registrando o estar vigilando en la red.[4]

TÍTULO NOVENO DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

CAPÍTULO II
ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMATICA

“ARTICULO 211 BIS 1. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de información protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.”

“ARTICULO 211 BIS 2. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa”.

ARTICULO 211 BIS 3.Al que estando autorizado para acceder a sistemas y equipos de informática del estado indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.
Al que estando autorizado para acceder a sistemas y equipos de informática del estado indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de cincuenta a cuatrocientos días multa.

“ARTÍCULO 211 4. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de las instituciones que integran el sistema

[4] www.delitosinformáticos.com.mx, 2002)

financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa".

"ARTICULO 211 BIS 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.
Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero".

"ARTICULO 211 BIS 6. Para los efectos de los artículos 211 BIS 4 y 211 BIS 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 BIS de este código".
"ARTICULO 211 BIS 7. Las penas previstas en este capítulo se aumentaran hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno".

Cosa que no sucede o no se sigue conforme a la ley pues la mayoría de las veces los delitos que se llegan a cometer son en grandes empresas por parte de los empleados en su caso de confianza por tener estos el acceso directo a este tipo de información y que inclusive llevan la quiebra económicamente hablando. La mayoría de las veces no se sanciona o castiga al culpable por alegar que no se tiene información ni conocimiento de quien delinquió.

2.3 Regulación Federal de Protección al Consumidor.

La privacidad y la protección de datos personales constituyen elementos importantes en las distintas modalidades del comercio electrónico, pero particularmente han adquirido mayor relevancia al momento en que los consumidores llevan a cabo transacciones comerciales por medios electrónicos; compras en Internet o intercambio de datos e información entre usuarios, empresas y gobiernos en la red.

El marco jurídico del comercio electrónico en México es relativamente reciente, sin embargo, la protección de datos personales ya se encuentra regulada en la Ley Federal de Protección al Consumidor y contempla la posibilidad de que los proveedores y consumidores puedan celebrar transacciones a través de medios electrónicos, pero al llevarse a cabo en la práctica las cosas cambian y más cuando se realiza en el comercio informal donde no se tiene los medios para defenderse cuando no nos venden lo que se nos ofrecía o llega a venir en malo estado, o ni siquiera se nos entrega lo que compramos por internet y este ya se había pagado.

CAPÍTULO VIII BIS
DE LOS DERECHOS DE LOS CONSUMIDORES EN LAS TRANSACCIONES EFECTUADAS A TRAVES DEL USO DE MEDIOS ELECTRÓNICOS, ÓPTICOS O DE CUALQUIER OTRA TECNOLOGÍA.

> **"ARTICULO 76 BIS**. Las disposiciones del presente capitulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:
> II. El proveedor utilizara alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informara a este, previamente a la celebración de la transacción, de las características generales de dichos elementos."

En este artículo se logra dejar en desventaja al consumidor hasta cierto punto toda vez que para realizar operaciones electrónicas como lo es el comercio electrónico proporciona parte de sus datos personales para que estas se puedan efectuar y quienes solicitan este tipo de información son los proveedores pudiendo hacer operaciones ilícitas con el uso de esta. También puede ser el caso de que un hacker acceda a páginas de compras por internet afectando tanto a los dueños de este tipo de comercio como a los clientes de las mismas y por consecuencia a toda información confidencial.

2.4. LEY FEDERAL DE PROTECCIÓN DE LOS DATOS PERSONALES. (PROYECTO)

Esta fue la primera iniciativa en relación con el tema de privacidad y protección de datos personales que se originó en la Cámara de Diputados del Congreso

de la Unión y fue presentada en septiembre de 2001, por el diputado Miguel Barbosa Huerta del Grupo Parlamentario del Partido de la Revolución Democrática (PRD) ante la LVIII Legislatura y publicada en la Gaceta Parlamentaria al día siguiente, fue presentad el proyecto como tal por el senador Antonio García Torres y aprobada en el Senado en abril de 2002 y publicada en la Gaceta Parlamentaria en septiembre del mismo año.

El proyecto se formuló precisamente en virtud a la ausencia de un marco jurídico de esta naturaleza en México, se buscó primeramente que el marco fuera protector y que por otro lado se otorgasen los instrumentos necesarios para hacer valer los derechos inherentes a esa tutela. La protección jurídica que planteamos fue para proteger valores como el honor, o bien la intimidad de las personas y por ende la repercusión familiar que este pudiere tener y el llamado *habeas data,* como la acción procesal que permite al ciudadano defender su derecho al respeto y a su vez el acceso a su información personal, a continuación describimos aspectos importantes del proyecto:

RESPECTO AL ÁMBITO DE APLICACIÓN

El ámbito de acción y aplicación de la ley fue pensado para regular tanto a la bases de datos públicas como privadas, ya sea controladas por personas físicas o jurídicas, que yacen en ellas o bien a todo uso posterior de los mismos (artículo 2° del proyecto) y los sujetos regulados son los que manejan los datos en cuestión así como los terceros que los ceden. Así mismo se planteó establecer regímenes de excepción en atención de la naturaleza de los archivos y las dependencias de que se trata y por ello la iniciativa marca que sean las propias dependencias las que lleven su regulación especial. La ley define lo que es archivo o base de datos, así como el tratamiento de los mismos. Se establecen principios rectores como la licitud que debe prevalecer en todo momento así como la finalidad que deber perseguir los mismos no contraviniendo a la ley y la moral, o bien principios especiales cuando se trate de datos sensibles o los relativos a condenas o sanciones penales.
A continuación se establecen los principios establecidos por la ley.

a) EL PRINCIPIO DEL CONSENTIMIENTO EN EL PROYECTO.

La ley establece el principio del consentimiento (artículos 27 y 28), es decir, solo se pueden recolectar datos personales destinados al reparto de documentos, publicidad, venta directa o bien cuando se traten de encuestas de opinión, investigación científica u otras actividades análogas, mediante el previo consentimiento del titular de esos datos. Se establece, que al recolectar previo consentimiento del titular, se deben destinar los datos al objeto exclusivo que originó la recolecta.

En materia de cesión de datos personales rige el mismo principio, previendo que la cesión se hará a persona con interés legítimo, informando de manera cabal sobre la identidad del cesionario y la finalidad que persigue la cesión. Así mismo se permite que se revoque la cesión, mediante una notificación al titular del archivo, registro, base o banco de datos. Sin embargo, el proyecto permite que no se requerirá del consentimiento cuando la propia ley así no lo exija, se realice entre dependencias y organismos públicos y el registro conste que la información en cuestión sea de consulta pública y gratuita.

b) DERECHO DE ACCESO A LOS DATOS PERSONALES Y SU RESPECTIVA MODIFICACIÓN.

El proyecto de ley, como podemos observar no solo en éste sino en muchos otros y en general en la legislación comparada, establece un derecho de acceso a la información que le atañe, por regla general al titular de los datos personales, lo que le permite tener un acceso a su información y se pueda dar un control diferido a los particulares frente a los titulares de las bases de datos. Esto conlleva a que, conforme al proyecto, pueden solicitar la inclusión, complementación, rectificación, actualización, reserva, suspensión o bien la cancelación de los datos que les conciernen a las personas. Este derecho, al ser ejercido, obliga a los titulares de las bases o bancos de datos a llevar a cabo estas acciones solicitadas por los particulares, informando al interesado de manera del tratamiento realizado.

Así mismo, el proyecto incluye la facultad a los titulares de pedir informes de los datos personales que le conciernan y obren en archivos, registros bases o bancos de datos públicos o privados que se destinen a proveer informes.

DEL INSTITUTO FEDERAL DE PROTECCIÓN DE DATOS PERSONALES

En el capítulo tercero se establecía la estructura, organización y constitución de lo que inicialmente habíamos previsto, el llamado Instituto Federal de Protección de Datos Personales, como un organismo público descentralizado con personalidad jurídica, patrimonio propio y autonomía para la realización de su finalidad, que ejercería el control de los responsables de los registros, bancos o bases de datos personales, a quienes podría sancionar. Actualmente en el proceso legislativo en el que se encuentra, la instancia de control será el que establezca la Ley Federal de Acceso a la Información Pública Gubernamental.

Es de destacarse que el Instituto Federal de Protección de Datos Personales se concibió como una instancia reguladora o de control, que debería ser finalmente instalada por el Ejecutivo Federal, por lo que queda en suspenso la aceptación o rechazo definitiva del Instituto que previmos.

DE LA ACCIÓN PROTECTORA DE LOS DATOS PERSONALES.

Se regula la acción protectora de los datos personales o *habeas data*, con la finalidad de conocer los datos personales almacenados en archivos públicos o privados destinados a proporcionar informes o bien en los casos en que se presuma falsedad, inexactitud, falta de actualización, omisión, total o parcial, o ilicitud de la información de que se trata, para exigir su rectificación, actualización, complementación, etcétera.

Pueden ejercitarla el afectado o sus representantes legales en contra de los responsables y usuarios de bancos de datos públicos y de los privados destinados a proveer informes. El juzgador competente son los de Distrito del domicilio del actor o bien del domicilio del demandado.

El procedimiento de la acción protectora de datos que pueden ejercitar los interesados es una tramitación sencilla y rápida, congruente con su objeto: la protección eficiente y eficaz de los derechos de los interesados.

EL PROCESO LEGISLATIVO DEL PROYECTO.

El proyecto de ley fue presentado el 14 de febrero 2001 en la Comisión Permanente del primer año legislativo de la presente legislatura del Congreso General de los Estados Unidos Mexicanos, turnándose a las comisiones de Puntos Constitucionales y Estudios Legislativos de la Cámara de Senadores. Después del análisis respectivo, se aprobó el 30 de abril de 2002 pasando para sus efectos constitucionales a la Cámara de Diputados el mismo día, la que iniciando el siguiente periodo ordinario de sesiones con fecha 5 de septiembre del mismo año, por conducto de su Mesa Directiva, turnó para su estudio y análisis a la Comisión de Gobernación de la Cámara de Diputados, donde se encuentra actualmente en estudio.
Durante el proceso legislativo se han tomado a consideración las opiniones de diversos sectores y grupos, como lo son las empresas de mercadotecnia, opiniones de consultores internacionales, el Banco de México, empresas privadas, instituciones de crédito, comentarios de juristas, que seguramente muchas de ellas serán incorporadas en el proyecto final.[5]

Frente a esta situación, será necesario encontrar un balance apropiado para la adopción de un esquema regulatorio bien estructurado, que combine programas de regulación del sector privado y propuestas de los sectores público y académico, protegiendo en la medida de lo posible, las garantías constitucionales de los individuos de libertad y privacidad, sin inhibir el desarrollo del comercio electrónico en México.[6]

Cabe mencionar que también existen organismos como la OCDE, la cual es una Organización para la Cooperación y el Desarrollo Económico, de carácter multilateral que ha elaborado importantes lineamientos y políticas sobre privacidad y protección de datos personales y que entre sus tantas funciones

[5] Senador Antonio García Torres, material no impreso.
[6] WWW. enterate.unam.mx/artículos,2006/enero/robo/html

esta el elaborar guías o lineamientos. Las Guías de la OCDE que regulan la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales del 23 de Septiembre de 1980 contienen ocho principios complementarios de aplicación nacional que son considerados como los estándares mínimos a seguir para la obtención, el procesamiento de datos y el libre flujo transfronterizo de datos para los sectores público y privado.

Los ocho principios de aplicación a nivel nacional son los siguientes:

1. El principio de "Límite de obtención", consistente en la imposición de límites para la obtención de datos personales mediante medios apropiados y legales haciéndolo del conocimiento y obteniendo el consentimiento;

2. El principio de "Calidad de los datos", consistente en la importancia de asegurar la exactitud, totalidad y actualización de los datos;

3. El principio del "Propósito de descripción", consistente en especificar el propósito de recabar información en el momento en el que se lleva a cabo la recolección y el subsecuente uso limitado del cumplimiento de dicho propósitos u otros que no sean incompatibles con aquellos propósitos especificados en cada ocasión;

4. El principio del "Límite de uso", consistente en no divulgar los datos personales o aquellos utilizados para propósitos distintos a los contemplados en el principio anterior, excepto:

- El consentimiento sobre la materia de datos;
- Mediante una autoridad contemplada en ley.

5. El principio de "Protección a la seguridad", consistente en proteger los datos personales e información, mediante mecanismos razonables de seguridad en contra de riesgos tales como pérdida, acceso no autorizado, destrucción, utilización, modificación o divulgación de datos;

6. El principio de "Imparcialidad", consistente en establecer políticas generales de imparcialidad sobre desarrollos, prácticas y políticas con respecto a los

datos personales, asegurando la transparencia en el proceso de obtención de información y estableciendo los propósitos para su utilización;

7. El principio de "Participación Individual", consistente en el derecho que tiene un individuo de: obtener del controlador de datos la confirmación de tener o no los datos del individuo; que el controlador de datos se lo haya comunicado en un tiempo y forma razonable; obtener respuesta del controlador de datos si una solicitud le ha sido negada y tener la posibilidad de impugnarla; tener la posibilidad de impugnar datos personales y si la impugnación resulta exitosa solicitar que los datos sean eliminados, modificados, rectificados o complementados; y

8. El principio de "Responsabilidad", consistente en la responsabilidad del controlador de datos de cumplir efectivamente con medidas suficientes para implementar los siete principios anteriores

2.5. Regulación Federal del Derecho de Autor.

El objeto de protección no es, el almacenamiento de obras, recopilaciones o partes de la misma, con una ordenación determinada que permita su búsqueda y posterior recuperación de una forma más adecuada, sino que se trata de todo el procedimiento de creación de una base de datos y el resultado del mismo, en cuanto a contenido, análisis, almacenamiento, clasificación, selección, ordenación y asociación de conceptos y unidades de información que caracteriza a una obra resultante la propia base de datos, como una creación intelectual y propia de su autor, esto es, el objeto de la protección es la base de datos que constituya una creación intelectual de su autor.

CAPÍTULO IV.

DE LOS PROGRAMAS DE COMPUTACIÓN Y LAS BASES DE DATOS.

> **“ARTICULO 107**. Las bases de datos o de otros materiales legibles por medio de maquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedaran protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos”.

> **“ARTICULO 108**. Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años”.
>
> **“ARTICULO 109**. El acceso a información de carácter privado relativa a las personas contenidas en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.
>
> Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos”.
>
> **“ARTICULO 110**.El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:
>
> I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;
> II. Su traducción, adaptación, reordenación y cualquier otra modificación;
> III. La distribución del original o copias de la base de datos;
> IV. La comunicación al público, y
> V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo”.

En los artículos 107 al 110 nos habla desde las obras que se protegen hasta el plazo para proteger a las bases de datos, no estoy de acuerdo en que nada más se debe de proteger a la obra y no a los datos pues los datos son importantes de ahí la importancia de ubicar a los creadores de las mismas y que si llegase a ocurrir un conflicto se puedan checar las bases y resolver cualquier duda. En cuanto al lapso yo considero que debería ser menor toda vez que todo avanza rápidamente y mas en materia tecnológica entonces podría ser una forma mas factible de tener la información actualizada.

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

No obstante que el fin de esta Ley es garantizar el acceso a los particulares a la información en posesión de los órganos del Estado, es una norma

determinante en materia de protección de datos personales debido a que en los archivos públicos se encuentra una gran cantidad de información que constituyen a los mismos aportados por los particulares y que requieren de protección. Sin embargo la protección de la información que esta Ley prevé va más allá de los datos personales toda vez que existe información que puede corresponder a personas públicas o privadas, morales o físicas o al Estado, las cuales en ocasiones es conveniente mantenerse en secreto debido a que su publicación puede traducirse en un perjuicio irreparable de alguna de éstas, entre estos tipos encontramos la información considerada reservada y la información confidencial.

Capítulo IV

Protección de datos personales

"Artículo 20. Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:

I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el Artículo 61;

II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61;

IV. Procurar que los datos personales sean exactos y actualizados;

V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y

VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado".

"Artículo 21. Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo

que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información".

"Artículo 22. No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:

I. (Se deroga).

Fracción derogada DOF 11-05-2004

II. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;

III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;

IV. Cuando exista una orden judicial;

V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y

VI. En los demás casos que establezcan las leyes".

"Artículo 23. Los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlo del conocimiento del Instituto o de las instancias equivalentes previstas en el Artículo 61, quienes mantendrán un listado actualizado de los sistemas de datos personales".

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

La entrega de los datos personales será gratuita, debiendo cubrir el individuo únicamente los gastos de envío de conformidad con las tarifas aplicables. No obstante, si la misma persona realiza una nueva solicitud respecto del mismo sistema de datos personales en un periodo menor a doce meses a partir de la última solicitud, los costos se determinarán de acuerdo con lo establecido en el Artículo 27.

"Artículo 25. Las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales. Con tal propósito, el interesado deberá

entregar una solicitud de modificaciones a la unidad de enlace o su equivalente, que señale el sistema de datos personales, indique las modificaciones por realizarse y aporte la documentación que motive su petición. Aquélla deberá entregar al solicitante, en un plazo de 30 días hábiles desde la presentación de la solicitud, una comunicación que haga constar las modificaciones o bien, le informe de manera fundada y motivada, las razones por las cuales no procedieron las modificaciones".

"Artículo 26. Contra la negativa de entregar o corregir datos personales, procederá la interposición del recurso a que se refiere el Artículo 50. También procederá en el caso de falta de respuesta en los plazos a que se refieren los artículos 24 y 25 de la misma ley".

CAPÍTULO TERCERO

CRÍTICA

Es importante destacar que, en materia de Internet el dueño de una base de datos (bancos, compañías de tarjetas de crédito, empresas de telemercadeo, oficinas de gobierno, por nombrar solo algunas) debe permitir a toda persona verificar y, de ser necesario, corregir cualquier información sobre ella. Asimismo, una persona puede prohibir el uso de su información personal en una base de datos.

Se ha presentado un acceso ilegal a todo sistema informático realizado dolosamente y sin el permiso del titular, incluida la figura del hacking, lo cual también provoca una interceptación ilegal por medios técnicos de transmisiones de datos informáticos de carácter privado, desde o dentro de un sistema informático.

También se ha interferido datos de manera intencional, para provocar daños, eliminar, deteriorar, alterar o suprimir datos de carácter personal, el caso de interferir el sistema cuando de manera intencional obstaculizan el correcto funcionamiento de un sistema informático o el mal uso de la información personal para cometer delitos informáticos mediante una clave o código de acceso para ingresar a la misma

3.1. SEGURIDAD EN INTERNET RESPECTO A LAS BASES DE DATOS PERSONALES

En internet el tema de la seguridad es enormemente complejo y extenso, complejo, toda vez que la clasificación categórica exige una tarea de selección que incluye el análisis de varios componentes, como lo son la fuente del ataque, el objeto del ataque, las calidades de los atacantes y los atacados, y la diferenciación entre ataque a la seguridad y a la privacidad y extenso, porque involucra la tarea de prever defensas dirigidas a los bienes jurídicos

tradicionalmente dignos de protección, e implica diseñarlas para aquellos que por su sola condición de nuevos carecen de importancia.[1]

En México, es necesario reconocer la importancia de Internet como un nuevo medio de comunicación de tecnología avanzada. Además, debe fomentarse la defensa del derecho de autodeterminación informativa a través de:

- El reconocimiento de que cada individuo tiene derecho a acceder a la información personal que le afecte, especialmente la de bancos de datos informatizados.
- El reconocimiento de que cada individuo tiene derecho a controlar, de manera razonable, la transmisión de la información personal que le afecte.
- Para garantizar el derecho a la intimidad individual las leyes deben regular la limitación de tiempo en que deba conservarse la información personal en la base de datos; la definición de los objetivos de uso de esa información en el inicio del procesamiento de datos; garantizar la calidad de los datos personales, su veracidad, integridad y actualidad, y la prohibición de la revelación de datos personales.[2]

Cosa que no se lleva a cabo pues la mayoría de las veces cuando nos vemos afectados en nuestra esfera personal las autoridades no nos auxilian o simplemente las personas que controlan las bases de datos no cumplen con la finalidad de las mismas y muchas veces ya ni se cercioran de que la información se actualize.

3.2. Seguridad Jurídica.

La seguridad jurídica es uno de los aspectos menos tratados por los juristas. Sus problemas de definición derivan de que es uno de los campos donde se dan mayores situaciones de ambigüedad.

---

[1] TELLEZ VALDEZ, JULIO "Derecho Informático", 3era Edición, Ed. McGraw Hill, México 2004

[2] BARRIOS GARRIDO, Gabriela, MUÑOZ DE ALBA MEDRANO, Marcia y PEREZ BUSTILLO, Camilo, "Internet y Derecho en México", Ed. McGraw Hill, México 1998, págs. 52 y 53

No obstante estas cuestiones, diremos que su concepción se basa en la esperanza o confianza de los ciudadanos en la función ordenadora del Derecho, por lo que es necesario darles protección. Dicha esperanza no puede, por tanto, quedar al libre albedrío del Poder o de otros particulares: el Derecho tiene que estar a disposición de los ciudadanos de manera incuestionable, segura.

En todo caso, la seguridad jurídica no se predica del conocimiento de la regulación de tal o cual norma específica o de sus consecuencias, a través fundamentalmente de su previa publicación, sino, sobre todo, por precisarse una buena estructura del Derecho, la ausencia de arbitrariedad y un grado cierto de previsibilidad, con el fin justo de dar esa confianza a los ciudadanos. A esto se le unen el poseer una cierta autonomía, objetividad y racionalidad; en definitiva, resguardar el ordenamiento jurídico de los defectos de la sociedad humana (principalmente del abuso del poder).

3.3. Peligros para la seguridad Jurídica.

Los peligros técnicos que son generados por redes abiertas tiene repercusiones directamente en el ámbito jurídico, toda vez que si consideramos que el derecho, como ciencia ordenadora de las relaciones sociales debe precisar consecuencias jurídicas a raíz de la utilización de determinadas herramientas informáticas o de la aceptación de una obligación electrónica.

3.3.1 Identificación y Autenticación.

En internet resulta más fácil realizar falsificaciones de identidades y, sin la utilización de ciertas herramientas tecnológicas, nos es imposible estar seguros de la identidad de un usuario, no obstante si lográramos identificarlo se originaría un nuevo inconveniente que es la necesidad de generar un marco legal que permita la autenticación de ciertos elementos que como en este caso sería una firma que vendría a ser la de dicho usuario para que otorgue efectos jurídicos a su declaración de voluntad. Dichos marcos legales desarrollados por los estados se centran, básicamente en dos aspectos:

- Leyes que castigan delitos cometidos por medio de la red, y
- Leyes que permiten la creación y utilización de firmas y certificados digitales.

La autenticación es lo acreditado de cierto y positivo por los caracteres, requisitos o circunstancias que en ello concurrenla obtienen los sistemas seguros verificando la información que el usuario brinda comparándola con lo que el sistema conoce acerca de él. El método para lograr dicha autenticación por parte del usuario es demostrando que pose cierta información esencial y confidencial a través de una contraseña o clave denominada “pastor”, existen otros métodos como lo son: la posesión de un objeto esencial y confidencial como una llave o tarjeta, la demostración de alguna característica biométrica como el escaneo de la retina, o la evidencia de que un tercero de confianza ha autenticado la identidad de la persona en sí.

3.3.2 Autorización y Control de Acceso.

Toda información que se transmite debe ser protegida para que no se altere o conozca mediante terceros, surgiendo la necesidad de realizar un control de acceso de usuarios, para que la información brindada o proporcionada solo pueda ser accedida por personas autorizadas. Una vez verificada la identidad de la persona se controle el acceso a la red. Obviamente en la realidad los que manejan las bases de datos también pueden acceder a la información y por ellos es que muchas veces se empiezan a dar los chantajes, los fraudes y otros delitos.

Dichos controles de acceso otorgan a los usuarios ciertos privilegios o permisos para acceder a recursos ofrecidos mediante la red, como lo son la creación o destrucción de la información, adición, borrado o modificación del contenido, entre otros y dichos privilegios a su vez pueden ser controlados por un simple usuario mediante la utilización de una lista de control de acceso, figurando todos los usuarios autorizados obviamente al sistemas

3.3.3 Integridad de los Datos.

Es uno de los aspectos más importantes en la realización de negocios mediante redes cuya finalidad entre otras es la de garantizar que todo dato proporcionado llegue a su destinatario sin sufrir alteración alguna. Entiéndase por integridad el garantizar que la modificación de la información y de los programas se realice exclusivamente de manera específica y autorizada, así como los datos presentados no se alteren o eliminen.
Este aspecto está vinculado con modificaciones de la información transmitida, por lo tanto los cambios en la misma que los servicios de integridad que protegen incluye adición, borrado y reorganización de partes de la información.

3.3.4 Confidencialidad de los Datos.

Se debe de asegurar la confidencialidad de toda información proporcionada o transmitida para que en un momento dado se pueda realizar una transacción u operación en internet, característica imprescindible y que ha merecido protección a nivel constitucional. La confidencialidad de los datos se refiere a la transmisión de datos e información de carácter secreta así como la protección del acceso no autorizado a dicha información y la confidencialidad debe a su vez garantizar dos aspectos:

- La información no puede ser leída, copiada o modificada o revelada sin la debida autorización.
- Comunicaciones entre redes no pueden ser interceptadas.

3.3.5. Disponibilidad de los datos.

Todo usuario debe de tener la posibilidad de acceder a su información, los mecanismos de seguridad buscan proteger esa información de toda acción que realice alguna persona ajena a la misma, pero es fundamental que los datos se encuentren disponibles para uso propio. Este criterio implica permitir el acceso continuo de los usuarios autorizados a la información así como a los recursos.[3]

[3] www.sre-gob/mx/transparencia/info_relevante/basesdedatos.htm

3.4. Requisitos esenciales para alcanzar la seguridad jurídica.

Estos son los siguientes:

a. Identificación de los usuarios que acceden ,
b. Imposibilidad fáctica de invasión de identidad,
c. Certeza de comunicación inalterable, y
d. Registración con validez probatoria.

3.5. Métodos de Protección.

La informática ha desarrollado varios métodos de protección para contrarrestar los problemas de la inseguridad de las redes abiertas, dichos métodos pueden clasificarse en diversas áreas y se originaron a partir de ciertos hechos técnicos informáticos que han logrado la reacción de la ciencia jurídica, estableciendo reglas claras sobre los derechos y deberes de cada parte.

3.6. Amenazas al Sistema y su Protección.

Las redes abiertas generan un ambiente propicio para estimular los ataques y amenazas de terceros, definiendo por amenaza una condición del entorno del sistema de información, ya sea persona, maquina, suceso o idea, que dada una oportunidad pueda dar lugar a que se produjese una violación de la seguridad como lo es la confidencialidad, la integridad, la disponibilidad de la misma, caso de que pese a la implementación de claves o contraseñas e inclusive candados para efectos de información importante han logrado traspasarse o romperse por gente cuya habilidad en el uso de las computadoras y más aun del internet no tiene limite ni freno alguno.[4]

3.7. Políticas de información.

Luego de analizar los problemas de inseguridad más frecuentes que presentan las redes abiertas y los problemas generados por este tipo de comunicaciones,

[4] Ver anexo 2

se debe considerar los puntos a tomar en cuenta para desarrollar una política de información.

En primer lugar se tomaran en cuenta todos los recursos que han de protegerse , se debe definir un proceso para poder identificar a quien se le permite el acceso a la información de carácter confidencial y privada así como también es sumamente importante controlar el sistema y actualizarlo con frecuencia, tomando en cuenta que se generan nuevos peligros constantemente.

3.8. Mecanismos de seguridad para usuarios y servidores.

Los peligros que se encuentran en una red abierta trae aparejado el desarrollo de una serie de mecanismos para restringir el acceso a los sistemas y garantizar que solo las personas autorizadas puedan accesar a ellos, cada mecanismo tiene diferente objetivo dependiendo de la forma en cómo se les analice desde la óptica del servidor o del usuario. Los desarrollados para garantizar la seguridad del usuario tienen por fin identificar con exactitud a la persona que está ingresando o accesando al sistema. Por otro lado, los que se preocupan por la seguridad del servidor buscan prevenir que sus sistemas sean atacados externa o internamente.

Los mecanismos de seguridad basados en el usuario son:

a) Certificados digitales: Son certificados emitidos por autoridades de certificación que garantizan la identidad de la persona certificándola mediante determinada firma digital donde la persona manifiesta su voluntad.
b) Tarjetas inteligentes: Son tarjetas que permiten al poseedor de la misma acceder a cierta información y se utilizan para ingresar al sistema o para acceder a ciertas secciones confidenciales. Las hay de tres tipos:

    1. De contacto: Estas necesitan ser insertadas en un lector
    2. Sin contacto: Basta con que se les acerque al lector para que intercambien datos, y

3. Combinadas: agrupan las funciones de las tarjetas con o sin contacto.

c) Identidad biométrica: Método de identificación automática de personas que está basado en características físicas o comportamientos personales, dicho sistema puede utilizar huellas dactilares, escaneo de retinas, a pesar de que confiere un mayor grado de confiabilidad, todavía no ha sido muy utilizado

Los principales mecanismos de seguridad basados en el servidor son:

a) *"Firewall":* Estos sistemas también son conocidos como cortafuegos y protegen a redes confiables que implican diferentes riesgos. Impide el acceso a ciertos sistemas que se encuentran conectados en Internet, dándose la posibilidad de especificar de donde provienen los usuarios y que servicios se les permite ver.
b) Protección del servidor: Se debe vigilar que los *hackers* no accedan a las bases de datos protegidas y así cometer actos ilegales, para poder identificarlos es necesario efectuar copias de seguridad de los archivos de registro y asegurarse de que los servicios y aplicaciones se generan correctamente.
c) Protección contra ataques desde el interior: Se debe proteger al sistema frente a ataques internos sobre todo por empleados que utilizan la contraseña raíz, ocasionando daños directos o alterando la seguridad. Esto se puede evitar mediante un control de autorizaciones a nivel interno.

3.9**Seguridad informática.**

Frente al poder informático la idea de un secreto individual y de privacidad debe consagrar, en todo ordenamiento jurídico la libertad de cada individuo a mantener secreta, por razones o necesidades de diversa índole, aquella esfera íntima que ha tenido que hacer del conocimiento de otra persona. El concepto informático de privacidad no está basado en la idea de que el hombre puede apegarse a su esfera privada. La base jurídica es más amplia, es el derecho de

la persona a conservar su autonomía, su identidad. El concepto de vida privada, en relación con la informática, tiene un doble significado. Por un lado la protección de la vida privada, estricto sentido, se refiere al problema de la información sensible, definida como aquella relativa al origen racial, a las opiniones públicas, religiosas y membrecías sindicales, información que no puede ser recopilada ni procesada electrónicamente salvo que exista autorización expresa del interesado; por el otro lado, el manejo y registro de otro tipo de información puede causar también atentados a la vida privada, pero en relación con el ámbito social al que pertenece.[5]

Este tipo de seguridad son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del *hardware*, la pérdida física de datos personales y el acceso a los datos mismos por personas no autorizadas. Diversas técnicas sencillas pueden dificultar la delincuencia informática. Por ejemplo, el acceso a información confidencial puede evitarse destruyendo la información impresa, impidiendo que otras personas puedan observar la pantalla del ordenador o computadora, manteniendo la información y los ordenadores bajo llave o retirando de las mesas los documentos sensibles. Sin embargo, impedir los delitos informáticos exige también métodos más complejos.

El mayor problema que tienen que resolver las técnicas de seguridad informática es el acceso a datos personales no autorizado por un *hacker* quien es denominado como un usuario muy avanzado que por su elevado nivel de conocimientos técnicos es capaz de superar determinadas medidas de protección. Internet, que cuenta con grandes facilidades de conectividad, permite a un usuario experto intentar de forma anónima, y a veces conseguir, el acceso remoto a una máquina conectada[6]. Las redes corporativas u ordenadores que también tienen datos confidenciales no suelen estar conectadas a Internet y en caso contrario, es decir, que exista una conexión se

[5] BARRIOS GARRIDO, Gabriela, MUÑOZ DE ALBA MEDRANO, Marcia y PEREZ BUSTILLO, Camilo, "Internet y Derecho en México", Ed. Mc Graw Hill, México 1998 págs.50, 51,52.
[6] TELLEZ VALDEZ, JULIO "DERECHO INFORMATICO", 3era Edición, Ed. McGraw Hill, México 2004 pag.149

utilizan los llamados cortafuegos, un ordenador situado entre las computadoras de una red corporativa e Internet, este cortafuegos impide a los usuarios no autorizados acceder a los ordenadores de una red, y garantiza que la información recibida no sea sustraída, alterada o modificada, cosa que muy difícilmente se cumple sino, no se presentarían casos de acceso ilícito a una base de datos personales y mucho menos delitos informáticos y de otra naturaleza a raíz de este.

CONCLUSIONES

PRIMERA.- Todo ordenamiento jurídico busca un sistema de protección de datos personales que sancione la utilización de los mismos por terceras personas, que sin autorización explícita del titular, puedan ser accesibles a otras personas y/o a una alteración por medio de equipos electrónicos, y provocar daños en lo personal, familiar, social o profesional del individuo al que se le transgredió su intimidad, situación que en la realidad es muy distinta pues no se aplican las leyes ni mucho menos las sanciones en estas establecidas y mucho menos se hace el intento por buscar todas estas anomalías.

SEGUNDA.- La protección de datos personales tiene una doble repercusión en las sociedades que utilizan Internet como un medio para transmitir, almacenar y procesar información ya que por un lado, exige obligaciones a quien tiene acceso y conocimiento de datos de carácter personal y por el otro, confiere derechos al titular de los datos, que puede ejercitarlos ante quien maneja esa información dentro de los límites legalmente establecidos, con el fin de controlar cómo, quién y para qué se tratan sus datos.

TERCERA.- En el caso específico de México, se tiene contemplada la Iniciativa de la Ley Federal de Protección de Datos Personales, presentada en febrero de 2001 a la Sesión de la Comisión permanente, que señala la necesidad de contener los efectos nocivos de las nuevas tecnologías sobre los tres derechos fundamentales de las personas: la autonomía, la inviolabilidad y la dignidad de la persona.

CUARTA.-El derecho positivo debe tutelar el derecho de acceso, rectificación, uso conforme al fin y prohibición de interconexión de archivos automatizados a las personas.

QUINTA.- Resulta conveniente, que en sectores altamente sensibles en donde la confidencialidad de la información de las personas es considerada primordial, como son el sector salud, bancario y laboral, se contemple la posibilidad de incluir aspectos puntuales sobre privacidad y protección de datos personales en el ámbito de sus respectivas leyes, reglamentos y ordenamientos.

SEXTA.- los principales apartados que llevan el alma del derecho a la protección de datos a través de Internet, o de cualquier medio electrónico, son los artículos primero, segundo y cuarto, de esta iniciativa de ley, de los que se ha preparado un breve extracto:

Artículo 1

1. Esta ley tiene por objeto asegurar que el trato de datos personales se realice con respeto a las garantías de las personas físicas.
2. Las disposiciones de esta ley también son aplicables, en lo conducente, a los datos de las personas jurídicas.
3. En ningún caso se podrán afectar los registros y fuentes periodísticas.

Artículo 2

1. Esta ley es aplicable a los datos de carácter personal que figuren en archivos, registros, bancos o bases de datos de personas físicas o jurídicas, públicas o privadas, y a todo uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado.

Artículo 4

IV. Tratamiento de datos: operaciones y procedimientos sistemáticos que tienen por objeto recolectar, guardar, ordenar, modificar, relacionar, cancelar y cualquiera otra que implique el procesamiento de datos, o su cesión a terceros a través de comunicaciones, consultas, interconexiones y transferencias.

Cabe señalar que Internet no es un complejo vacío jurídico, pero debe garantizarse la aplicación tanto de una legislación, así como la ejecución de conjuntos de normas que regulen el aspecto jurídico en la protección de datos.

La protección de datos en Internet es una obligación para quienes tienen contacto con datos de los usuarios y significa una garantía para éstos últimos. Sin embargo, este régimen de confianza debe estar basado en disposiciones legales sin importar la diferencia entre los distintos ordenamientos jurídicos de cada nación o de las diferentes soluciones tecnológicas que desde la industria del hardware y software se desarrollen para dar soluciones específicas a esta cuestión.

“BIBLIOGRAFIA.”

“Derecho y Control en Internet: La regulabilidad de Internet”
MOLES PLAZA, Ramón J.
ED. Ariel S.A.
España 2004

“Derecho e Informática”
GALINDO, Fernando.
ED. La Ley-Actualidad.
España 1998.

“Derecho e Informática; Informática Jurídica, Derecho de la Informática”
RIOS ESTAVILLO, Juan José.
UNAM Instituto de Investigaciones Jurídicas.
México 1997.

“Derecho Informático”,
TELLEZ VALDEZ, Julio
ED. MC Graw Hill.
ed. 3ª
México, 2004

“El uso de Internet en el Derecho”
ROJAS AMONDI, Víctor Manuel.
ED. Oxford.
Ed. 2ª
UNAM: Colección Estudios Jurídicos.
México 2001.

“Informática y Decisión Jurídica”
BARRAGAN, Julia.
ED. Fontamaria.
México 1994.

“Internet y Derecho en México”
BARRIOS GARRIDO, Gabriela
MUÑOZ DE ALBA MEDRANO, Marcia

PEREZ BUSTILLO, Camilo
ED. McGraw Hill.
México 1998.

“Manual de Derecho Informático”
DR. DAVARA RODRIGUEZ, Miguel Ángel.
ED. Aranzadi.
España 2004.

“LEGISLACIÓN”

- Constitución Política de los Estados Unidos Mexicanos.
- Código Penal Federal.
- Ley Federal del Derecho de Autor.
- Ley Federal de Protección al consumidor.
- Código de Comercio

FUENTES ELECTRÓNICAS

- www. nacpec.org/es/links/robo_identidad/index.htm
- www. enterate.unam.mx/artículos,2006/enero/robo/html
- www.sre-gob/mx/transparencia/info_relevante/basesdedatos.htm
- www.ssp.gob.mx/_c_programas/p_cibernetica/INDEX.htm
- www.delitosinformáticos.com.mx, 2002)

ANEXO 1

REGISTRO DE SISTEMAS DE DATOS PERSONALES

Nombre de la Unidad Administrativa	Servicios de Salud Mental Hospital Psiquiátrico Fray Bernardino Álvarez
Nombre del sistema de datos personales	Expedientes Clínicos
Objetivo del sistema	Tener un registro individualizado de los usuarios del servicio
Tipo de datos que contiene	Datos de características físicas, características emocionales, vida afectiva, vida familiar, domicilio, número de teléfono, estado de la salud física, estado de la salud mental, preferencia sexual y otras análogas que afecten su intimidad
Usos del sistema	Registro de información relevante para la atención médica
Datos del responsable del sistema	
Nombre completo	Dr. José Luis García Aguirre
Puesto	Jefe de la División de Servicios Auxiliares de Diagnóstico y Paramédicos
Domicilio	Avenida San Buenaventura y Niño de Jesús No. 2, Col. Tlalpan, Deleg. Tlalpan, C.P. 14000
Teléfonos	Tel: 5573-0387
Fax	Fax: 5573-0388
Correo E.	marspy@todito.com

*http://www.sre.gob.mx/transparencia/info_relevante/basesdedatos.htm

ANEXO 2

SISTEMA DE BASE DE DATOS PERSONALES

DIRECCIÓN GENERAL	NOMBRE	OBJETO	TIPO DE DATOS	USO QUE SE LE DA	UNIDAD ENCARGADA	RESPONSABLE
Instituto de los Mexicanos en el Exterior	Base de datos personales de los miembros del Consejo Consultivo del IME	Directorio Actualizado	Nombre, dirección, teléfonos, correo electrónico	Envío de información, convocatoria a reuniones, conferencias telefónicas	Dirección de Atención al Consejo Consultivo del Instituto de los Mexicanos en el Exterior	Luisa Medina Mora, Directora de Atención al Consejo Consultivo del IME R. Flores Magón Nº Col. Guerrero México, D.F., 06995 5117-4279
Instituto de los Mexicanos en el Exterior	Base de datos de dirigentes de comunidades mexicanas y de líderes de opinión en Estados Unidos	Directorio Actualizado	Nombre, dirección, teléfonos, correo electrónico	Envío de Boletín electrónico diario, envío de información especializada, invitaciones.	Dirección General Adjunta del Instituto de los Mexicanos en el Exterior	Lic. Juan Carlos Mendoza Sánchez, Director General Adjunto del IME R. Flores Magón Nº2 Col. Guerrero México, D.F., 06995 5117-4281
Unidad de Asuntos Culturales	Sistema de Registro para Becarios Mexicanos	Registro actualizado para ordenar y acceder a la información de estudiantes mexicanos becados por gobiernos extranjeros	Maneja cuatro campos principales: Ofrecimientos, Becarios, Área/nivel, y Situación.	Base de datos de estudiantes nacionales quienes realizan o han realizado estudios como becarios de terceros países.	Dirección de Intercambio Académico de la Unidad de Asuntos Culturales	Lic. Sean Carlos Cázares Ahearne Subdirector de Intercambio Académico Ave. Paseo de la Reforma 175 Col. Cuauhtémoc Del. Cuauhtémoc México, D.F., 06500 5782-4144

						Ext. 2713 y 2714
Unidad de Asuntos Culturales	Sistema de Registro de Becas para Extranjeros	Registro actualizado para ordenar y acceder a la información de Becarios extranjeros del Gobierno de México.	Maneja tres categorías principales: Becarios, Avances de Investigación e Histórico.	Acceso rápido y ordenado a la información requerida por la Dirección de Intercambio Académico.	Dirección de Intercambio Académico de la Unidad de Asuntos Culturales	Lic. Sean Carlos Cázares Ahearne, Subdirector de Intercambio Académico Ave. Paseo de la Reforma 175 Col. Cuauhtémoc Del. Cuauhtémoc México, D.F., 06500 5782-4144 ext. 2713 y 2714
Dirección General de Protección y Asuntos Consulares	Sistema de Información Consular (SIC)	Revertir el rezago existente en las Representaciones Consulares en materia de servicios de documentación.	Los módulos del SIC contienen los siguientes datos: nombre del individuo, lugar y fecha de nacimiento, edad, sexo, estado civil, domicilio, nombre de algún familiar y en algunos casos como el de la visa de alta seguridad, la nacionalidad.	Registro de datos a partir de cuatro módulos básicos:a. Libro Electrónico de Registro. b. Matrícula de Alta Seguridad. c. Pasaportes tipo libreta "E". d. Visa de Alta Seguridad.	Dirección General de Comunicaciones e Informática y Dirección General de Protección y Asuntos Consulares	Ministro Juan Miguel Gutiérrez Tinoco, Encargado de la Dirección General de Protección y Asuntos Consulares R. Flores Magón Nº 1, Anexo II, planta baja Col. Guerrero, México, D.F. 06995 5327-3153 Ing. Norman Levy Marks, Director General de Comunicaciones e Informática R. Flores Magón Nº 2, Nuevo Edificio Ala A, piso 2 Col. Guerrero, México,

						D.F., 06995 5117-2174
Dirección General de Protección y Asuntos Consulares	Sistema de Protección Consular (SPC	Proporcionar a las dependencias de la S.R.E. un sistema automatizado en red para el registro, atención y seguimiento de los casos de Protección a Mexicanos en el Exterior	Los datos son de carácter personal, corresponden a los nacionales mexicanos a quienes se proporciona asistencia consular en el extranjero, tales como: nombre, apellidos, fecha de nacimiento, entidad federativa de origen, domicilio, teléfono, asunto o problema que presenta, número de expediente y los seguimientos o gestiones realizados por la Representación Consular respectiva.	El uso de dichos datos sirve para ubicar de manera sistemática a las personas que requieren asistencia y protección consular en el exterior, o bien para localizar a sus familiares, con el propósito de hacer de su conocimiento la evolución de sus casos.	Dirección General de Comunicaciones e Informática y Dirección General de Protección y Asuntos Consulares	Francisco Javier Palmerín Romero, Director de Innovación Tecnológica R. Flores Magón Nº 2, Nuevo Edificio Ala A, piso 2 Col. Guerrero, México, D.F., 06995 5117-4265 Aníbal Gómez Toledo, Director de Protección a Mexicanos R. Flores Magón Nº 1, Anexo II, planta baja Col. Guerrero, México, D.F. 06995 5117-2136
Dirección General de Asuntos Jurídicos	Sistema Digitalizado para la Expedición de Documentos de Nacionalidad	Contar con información ágil, oportuna y sistematizada, para atender las solicitudes del público usuario en la materia	Nombre completo de los interesados; Lugar y fecha de nacimiento; Nacionalidad. Genero; Domicilio particular; Número telefónico; Profesión u ocupación; Estado civil;	Información sistematizada que se utiliza para la expedición de cartas de naturalización, así como de certificados y declaraciones de	Dirección de Nacionalidad y Naturalización	Lic. Irma García Mejía, Directora de Nacionalidad y Naturalización. R. Flores Magón Nº 1, Torre Anexo II, planta alta, Col. Guerrero, México,

			Nombre y nacionalidad del cónyuge; Lugar y fecha de matrimonio; Nombre y nacionalidad de los hijos; Lugar y fecha de nacimiento de los hijos; Nombre y nacionalidad de los padres; Bienes inmuebles en territorio nacional;	nacionalidad		D.F., 06995 5117-4250
Dirección General de Asuntos Jurídicos	Sistema de Información para Cartas Rogatorias y su Consulta Vía Internet.	Contar con una herramienta para el control y gestión de cartas rogatorias, que permita agilizar el proceso y proporcionar al interesado en forma ágil, eficiente y transparente el estado que guarda el trámite.	Este Sistema se compone de 7 carátulas de las cuales los datos se capturan en los siguientes apartados para su registro: Origen del documento: El número que se asigna en la Dirección General (DG) Fecha de ingreso Tipo de documento Nombre del Promovente y del Demandado. Remitente Autoridad exhortante Fecha de turno para su dictamen.	Atender en forma oportuna las solicitudes recibidas, a efecto de dar la debida atención al público usuario.	Dirección de Asistencia Jurídica.	Lic. Bertha Sánchez Miranda, Directora de Asistencia Jurídica. R. Flores Magón Nº 1, Torre Anexo II, planta alta, Col. Guerrero, México, D.F., 06995 5327-3157

			Antecedentes: Expediente interno Expediente del juzgado exhortante Tipo de juicio Oficios.- Esta carátula se utiliza para la actualización de datos. Número de oficio con el que se atendió. Fecha del oficio Observaciones (Pequeña síntesis del oficio de descargo) Observaciones generales. Se captura extracto del asunto.			
Dirección General de Asuntos Jurídicos	Sistemas Digitalizados para la Expedición de Permisos Artículo 27 Constitucional. Constitución de Sociedades	Contar con un sistema automatizado de las denominaciones autorizadas para la constitución de una sociedad mexicana y proporcionar un trámite de calidad con valor agregado, en forma ágil, eficiente y	Nombre del promoverte; Domicilio para oír y recibir notificaciones; Denominación solicitada en orden de preferencia; Régimen jurídico de la persona moral	Para la expedición de permisos para la constitución de sociedades y/o reformas a sus estatutos (cambio de denominación o razón social), evitando la duplicidad.	Dirección de Permisos Artículo 27 Constitucional.	Lic. Julio Alejandro Dorantes Hernández, Director de Permisos Artículo 27 Constitucional. R. Flores Magón Nº 1, Torre Anexo II, planta alta, Col. Guerrero, México, D.F., 06995

		transparente en su operación, con incorporación del mismo vía Internet.				5117-2208
Dirección General de Asuntos Jurídicos	Adquisición de inmuebles por extranjeros fuera de zona restringida	Mantener un control sistematizado, que permita establecer a que persona extranjera pertenece un bien inmueble ubicado fuera de zona restringida.	Número de folio; Nombre del solicitante y/o de su representante legal; Domicilio para oír y recibir notificaciones; Número de la delegación; Calidad migratoria; Nacionalidad: Tipo o forma de adquisición; Ubicación del inmueble adquirido; Superficie del inmueble; Número del documento migratorio.	Para la expedición de constancias en las cuales se tenga por aceptado el convenio de renuncia a que se refiere la fracción I, del artículo 27 Constitucional.	Dirección de Permisos Artículo 27 Constitucional.	Lic. Julio Alejandro Dorantes Hernández, Director de Permisos Artículo 27 Constitucional. R. Flores Magón Nº 1, Torre Anexo II, planta alta, Col. Guerrero, México, D.F., 06995 5117-2208
Dirección General de Asuntos Jurídicos	Constitución de fideicomisos	Contar con un control que permita establecer a que persona extranjera, a través de la figura del fideicomiso, se les ha autorizado el uso y aprovechamiento de un bien inmueble ubicado en zona restringida.	Fideicomisario; Fideicomisario substituto; Nacionalidad del fideicomisario; Tipo de cláusula; Nacionalidad substituto; Fideicomitente; Nacionalidad del fideicomitente; Cláusula; Bien materia del fideicomiso;	Para la expedición de permisos para la constitución de fideicomisos en zona restringida	Dirección de Permisos Artículo 27 Constitucional.	Lic. Julio Alejandro Dorantes Hernández, Director de Permisos Artículo 27 Constitucional. R. Flores Magón Nº 1, Torre Anexo II, planta alta, Col. Guerrero, México, D.F., 06995 5117-2208

			Domicilio del inmueble; Superficie del inmueble; Duración; Distancia del inmueble a la playa y/o frontera; Uso; Institución fiduciaria; Datos de inversión; Duración de la inversión.			
Dirección General del Servicio Exterior y de Personal	Sistema de base de datos del Servicio Exterior Mexicano	La administración del personal del Servicio Exterior Mexicano	Nombre, Apellido Paterno, Apellido Materno, RFC, CURP, Domicilio, Teléfono, datos de Estudios, datos de Escalafón, datos de Licencias, datos de Vacaciones, datos de Evaluaciones, datos de Actas Administrativas, datos de Acuerdos, datos de Menaje, datos de Importaciones, datos de Plantilla, datos de Seguros	Generar reportes, informativos como Escalafón, Licencias, Seguros, Evaluaciones, etc.	Dirección General Adjunta del Servicio Exterior Mexicano	María de Lourdes del Río Pesado Ave. Paseo de la Reforma Nº 175, piso 5, Col. Cuauhtémoc, México, D.F., 06500 5241-3369
Dirección General del Servicio Exterior y de Personal	Sistema de Nómina	Ejecución y proceso de los movimientos de personal local y del Servicio Exterior	Nombre, Apellido Paterno, Apellido Materno, RFC, Calle, Colonia, Entidad, CP,	Generar reportes, Recibos de Pago, Reportes al ISSSTE, Retenciones, SAR, y	Dirección General Adjunta de Personal	Carlos Garduño Aréizaga Ave. Paseo de la Reforma Nº 175, piso 6,

		Mexicano para el cálculo de Nómina	Clínica, Sexo, CURP, Delegación, Teléfono, datos de Percepciones y Deducciones, datos de Impuestos, datos de Incidencias, Fichas de Ingreso, Fichas de Bajas, datos del ISSSTE, datos del FOVISTE, datos de Seguros, datos de Plantilla	en general los productos de nómina		Col. Cuauhtémoc, México, D.F., 06500 5241-3373
Dirección General del Servicio Exterior y de Personal	Sistema Integral de Recursos Humanos (en implantación)	Proporcionar a la Secretaría de Relaciones Exteriores un mejor servicio interno, agilizar, dar seguimiento a los procesos de la institución, con el fin de mejorar continuamente los servicios de recursos humanos. Contar con un único repositorio de datos. Automatización de procesos	RFC, Región, País, Estado, Ciudad, CURP, Nombre, Apellido Paterno, Apellido Materno, Dirección, Código Postal, fecha de Nacimiento, Fecha de Ingreso, Estado Civil, Sexo, Talla, Estatura, Peso, Teléfono Celular, Correo Electrónico, datos de Licencias, datos de Vacaciones, datos de Evaluaciones, datos de Actas Administrativas, datos	Generar reportes, informativos como Escalafón, Licencias, Seguros, Evaluaciones, Recibos de Pago, Reportes al ISSSTE, Retenciones, SAR, en general los productos de nómina la administración del personal	Dirección General Adjunta de Personal	Manuel Martínez Núñez Ave. Paseo de la Reforma Nº 175, piso 6, Col. Cuauhtémoc, México, D.F., 06500 5782-4144 ext. 3293

			de Acuerdos, datos de Menaje, datos de Importaciones, datos de plantilla, datos de Sueldos, datos de Impuestos, datos de Incidencias, Fichas de Ingreso, Fichas de Bajas, Datos del ISSSTE, datos de FOVISTE, datos de Seguros			

www.salud.gob.mx/transparencia/datos_personales/sersame.doc+registro+de+sistemas+de+datos+personales