UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

ANÁLISIS JURÍDICO DE LA CALIFICACIÓN Y CLASIFICACIÓN DE DATOS PERSONALES QUE SEAN DE ACCESO A EMPRESAS PRIVADAS

SALVADOR RODRIGO CHINCHILLA SCHMID

GUATEMALA, ABRIL DE 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

ANÁLISIS JURÍDICO DE LA CALIFICACIÓN Y CLASIFICACIÓN DE DATOS PERSONALES QUE SEAN DE ACCESO A EMPRESAS PRIVADAS

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

SALVADOR RODRIGO CHINCHILLA SCHMID

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADO Y NOTARIO

Guatemala, abril de 2011

HONORABLE JUNTA DIRECTIVA
DE LA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

DECANO:	Lic. Bonerge Amilcar Mejía Orellana
VOCAL I:	Lic. César Landelino Franco López
VOCAL II:	Lic. Gustavo Bonilla
VOCAL III:	Lic. Luis Fernando López Díaz
VOCAL IV:	Br. Mario Estuardo León Alegría
VOCAL V:	Br. Luis Gustavo Ciraiz Estrada
SECRETARIO:	Lic. Avidán Ortiz Orellana

TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL

Primera Fase:

Presidente:	Lic. Héctor Marroquín Aceituno
Vocal:	Licda. Vilma Esperanza Perdomo
Secretario:	Lic. José Eduardo Cojulun

Segunda Fase:

Presidente:	Lic. Homero Nelson López
Vocal:	Lic. Marco Tulio Pacheco
Secretario:	Lic. David Sentes Luna

RAZÓN: "Únicamente el autor es responsable de las doctrinas sustentadas y contenido de la tesis" (Artículo 43 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales del Examen General Público).

LICDA. PEGGY IVONNE PALACIOS MÉNDEZ
ABOGADA Y NOTARIA
COLEGIADA 8,172

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Guatemala, C. A.

Guatemala, 03 de marzo de 2010.

FACULTAD DE CIENCIAS
JURIDICAS Y SOCIALES
RECIBIDO
14 ABR. 2010
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

Licenciado
Marco Tulio Castillo Lutin
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala

Licenciado Castillo Lutin:

En cumplimiento a la providencia dictada por la Unidad de Tesis, procedí a asesorar bajo mi dirección al estudiante SALVADOR RODRIGO CHINCHILLA SCHMID, para la elaboración de su trabajo de tesis denominada: "ANÁLISIS JURÍDICO DE LA CALIFICACIÓN Y CLASIFICACIÓN DE DATOS PERSONALES QUE SEAN DE ACCESO A EMPRESAS PRIVADAS". Por lo cual, manifestando que me fundamento en lo que indica el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, emito el siguiente dictamen:

El trabajo en mención, considero, en mi opinión, es altamente meritorio, advirtiéndose el empeño del autor en la investigación y en la construcción del marco teórico, como en el contenido científico y técnico de la misma que, nos muestra y sirve de aporte para un desarrollo abundante, en lograr entender la importancia del tema estableciendo que debe ser de sumo interés para el Estado desvirtuar y proteger el accionar de empresas, en la creación, uso y determinación en la materialización de información, que está desprotegida por un orden fiscalizador y público, que mantenga la integridad inherente en el acceso de la información de las personas, para poder crear un entorno de confianza al momento que cualquier individuo se manifieste en su entorno social.

LICDA. PEGGY IVONNE PALACIOS MÉNDEZ
ABOGADA Y NOTARIA
COLEGIADA 8,172

Por lo tanto, habiendo existido un trabajo de investigación razonable en la utilización de la metodología adecuada, de la utilización correcta de la técnica de abstracción bibliográfica a través de fichas que proporcionan abundantes aportes doctrinarios relacionados con el tema que, indudablemente complementan el trabajo, con una aceptación correcta en la redacción y, ortografía, así como la legislación correspondiente en derecho comparado; las conclusiones y recomendaciones fueron realizadas de forma apropiada en base a las averiguaciones encontradas durante la redacción del presente trabajo, de forma legal y doctrinaria, obteniendo así un aporte jurídico, científico y teórico valioso para la Facultad de Ciencias Jurídicas y Sociales y los profesionales del Derecho, complementado con textos suficientes para el apoyo de la investigación.

Por tanto, previo a haber realizado las correcciones correspondientes en el sentido de que sea admitido el trabajo propuesto como tesis de graduación del bachiller Salvador Rodrigo Chinchilla Schmid, hago constar que el mismo cumple con todos los requisitos legales, de forma y fondo establecidos en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público el cual establece literalmente "Tanto el asesor como el revisor de tesis, harán constar en los dictámenes correspondientes, su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, las conclusiones, las recomendaciones y la bibliografía utilizada, si aprueban o desaprueban el trabajo de investigación y otras consideraciones que consideren pertinentes."

Considero adecuado el trabajo de tesis y emito DICTAMEN FAVORABLE aprobando el trabajo de tesis titulado: "ANÁLISIS JURÍDICO DE LA CALIFICACIÓN Y CLASIFICACIÓN DE DATOS PERSONALES QUE SEAN DE ACCESO A EMPRESAS PRIVADAS".

Reitero mis muestras de respeto al señor jefe de la unidad de tesis, con la satisfacción de retribuir en algo a mi alma mater.

Licda. Peggy Ivonne Palacios Méndez
Colegiado número 8,172

Peggy Ivonne Palacios Méndez
Abogada y Notaria

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

Ciudad Universitaria, zona 12
Guatemala, C. A.

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Guatemala, C. A.

UNIDAD ASESORÍA DE TESIS DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, diecisiete de mayo de dos mil diez.

Atentamente, pase al (a la) LICENCIADA (A) JUANA MARÍA ESPAÑA PINETTA, para que proceda a revisar el trabajo de tesis del (de la) estudiante SALVADOR RODRIGO CHINCHILLA SCHMID, Intitulado: "ANÁLISIS JURÍDICO DE LA CALIFICACIÓN Y CLASIFICACIÓN DE DATOS PERSONALES QUE SEAN DE ACCESO A EMPRESAS PRIVADAS".

Me permito hacer de su conocimiento que está facultado (a) para realizar las modificaciones de forma y fondo que tengan por objeto mejorar la investigación, asimismo, del título de trabajo de tesis. En el dictamen correspondiente debe hacer constar el contenido del Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, el cual dice: "Tanto el asesor como el revisor de tesis, harán constar en los dictámenes correspondientes, su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, las conclusiones, las recomendaciones y la bibliografía utilizada, si aprueban o desaprueban el trabajo de investigación y otras consideraciones que estimen pertinentes".

LIC. MARCO TULIO CASTILLO LUTÍN
JEFE DE LA UNIDAD ASESORÍA DE TESIS

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FAC. DE C.C. J.J. Y S.S.
UNIDAD DE ASESORIA DE TESIS
GUATEMALA, C. A.

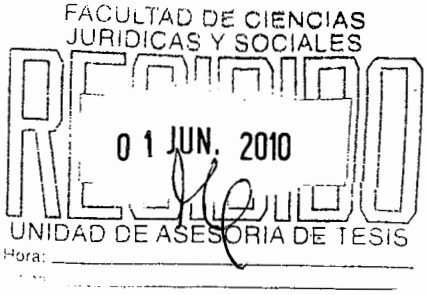
cc.Unidad de Tesis
MTCL/sllh.

OFICINA JURIDICA ESPAÑA

Licenciada Juana María España Pinetta

Abogada y Notaria

Guatemala, 24 de mayo de 2010.



Licenciado
Marco Tulio Castillo Lutín
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala

Licenciado Castillo Lutín:

Me place saludarle deseándole los correspondientes éxitos en ese Despacho y demás labores profesionales.

Por este medio en cumplimiento al nombramiento realizado a mi persona, como Revisor del trabajo de tesis del bachiller **SALVADOR RODRIGO CHINCHILLA SCHMID**, intitulado **"ANÁLISIS JURÍDICO DE LA CALIFICACIÓN Y CLASIFICACIÓN DE DATOS PERSONALES QUE SEAN DE ACCESO A EMPRESAS PRIVADAS"**. Me permito dictaminar respecto a la revisión del mismo en el siguiente sentido:

1. Se procedió a revisar el análisis, las teorías, metodología, hipótesis y aportaciones sustentadas por el autor, así como la estructura y el desarrollo de la investigación, las cuales se consideran atinentes a un trabajo de investigación de tesis de grado

2. La redacción y técnicas de investigación fueron adecuadas para el documento, de igual forma la información y bibliografía recopilada para su análisis y descripción fue trabajada y ordenada correctamente.

3. El trabajo desarrollado abarcó en su totalidad las distintas áreas y temas necesarios y vinculantes para probar la hipótesis planteada por el autor; destacando en sus conclusiones y aportando en las recomendaciones la importancia que persigue la Carta Magna en referencia a la igualdad de las personas y la protección a su intimidad, en lo que respecta a la publicidad de los datos personales esto en relación al acceso que empresas privadas puedan obtener y exigir a los particulares, y brindando como

alternativa y aporte académico, una investigación y análisis de fondo, tanto en orden legal como doctrinario sobre la calificación y clasificación de datos personales.

4. De la revisión practicada, se establece que el trabajo contiene una contribución científica importante no solo para la Universidad de San Carlos de Guatemala, sino para los actores políticos y académicos responsables del análisis de la coyuntura nacional y del planteamiento de soluciones a los problemas de trascendencia e impacto social.

5. El presente trabajo reúne los requisitos reglamentarios exigidos en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y el Examen General Público en la Universidad de San Carlos de Guatemala el cual literalmente establece "Tanto el asesor como el revisor de tesis, hará constar en los dictámenes correspondientes, su opinión respecto de contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, las conclusiones, las recomendaciones y la bibliografía utilizada si aprueban o desaprueban el trabajo de investigación y otras consideraciones que consideren pertinentes."

6. En consecuencia confiero **DICTAMINAR FAVORABLEMENTE** en el sentido que al ser cumplidos los requisitos previstos en dicho normativo, debe el bachiller sustentante ser sometido al examen público ante el Tribunal Examinador correspondiente para optar al grado académico de Licenciatura en Ciencias Jurídicas y Sociales.

Agradeciendo su atención a la presente y sin otro particular, me suscribo como su atenta y segura servidora.

Atentamente,

Licda. Juana María España Pinetta
Colegiado número 2817

Juana María España Pinetta
ABOGADO Y NOTARIO

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

Edificio S-7, Ciudad Universitaria
Guatemala, C. A.

DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, veintinueve de marzo del año dos mil once.

Con vista en los dictámenes que anteceden, se autoriza la Impresión del trabajo de Tesis del (de la) estudiante SALVADOR RODRIGO CHINCHILLA SCHMID, Titulado ANÁLISIS JURÍDICO DE LA CALIFICACIÓN Y CLASIFICACIÓN DE DATOS PERSONALES QUE SEAN DE ACCESO A EMPRESAS PRIVADAS. Artículos 31, 33 y 34 del Normativo para la elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.-

CMCM/sllh.

DEDICATORIA

A DIOS: Por darme la vida, cuidarme, amarme y darme todo lo que necesito; permitirme el día de hoy alcanzar uno de mis más grandes sueños, dándome fortaleza, esperanza y amor; llenándome de tantas bendiciones, siendo el motor que me impulsa para hacer todo lo que quiero, este logro es gracias a él y para él.

A MI PADRE: Sabino Salvador Chinchilla Chávez, por ser mi más grande inspiración en la vida y la persona quien más admiro, por motivar cada paso que doy con sus consejos y guía, por su gran amor y entrega, este logro es para ti y es el reflejo de tu gran esfuerzo, gracias por todo.

A MI MADRE: Alexandra Schmid González, por ser la mujer que más amo en mi vida y porque sin ella no fuera lo que soy, por todo su amor, cuidado, ternura, preocupación, consejos y oraciones, gracias por estar siempre a mi lado incondicionalmente, este triunfo es para ti.

A MI HERMANO: Andrés Alexander Chinchilla Schmid, por compartir conmigo todo el largo camino de mi vida y apoyarme en los momentos que más lo he necesitado de manera incondicional, por aconsejarme y preocupase por mí.

A MIS AMIGOS: A todos mis amigos que me apoyan y me han acompañado a lo largo de mi vida con sus consejos, amor, lealtad y ayuda; por la admiración que les tengo y por los momentos tan buenos que pasamos juntos.

A MIS PADRINOS: Por la gran admiración que les tengo y el apoyo incondicional que me han demostrado, por sus consejos y preocupación en cada situación de mi vida, estando presentes para apoyarme; por todo su cariño y amistad, gracias.

A: La tricentenaria Universidad de San Carlos de Guatemala y en especial a la Facultad de Ciencias Jurídicas y Sociales, por ser la más gloriosa de todas, haberme formado como profesional y por aportarle valores y principios a mi vida.

ÍNDICE

Pág.

Pág.

CAPÍTULO II

CAPÍTULO III

Pág.

CAPÍTULO IV

INTRODUCCIÓN

El sistema jurídico guatemalteco se ha caracterizado por regular conforme a las necesidades sociales que se han ido presentando a través del tiempo y como es costumbre se ha trabajado bajo parámetros ya construidos; es decir, sobre normativas que se han elaborado con anterioridad anticipándose a los hechos, actos y circunstancias que se pretenden regular, por lo que en la actualidad es evidente la falta de bases legales que busquen mantener la seguridad de las personas en relación a sus datos personales.

Los datos personales son medios a través de los cuales se engloban muchos ámbitos de la sociedad humana desde cómo se identifican, a qué grupo político pertenecen, religión, costumbres, hasta la económica que cada individuo posee, entre otras; asimismo, estos datos determinan hechos y circunstancias que son particulares de cada sujeto y deben ser protegidos atendiendo la seguridad de la intimidad de cada persona.

A través del tiempo se ha evidenciado la falta de seguridad jurídica en el manejo de la información que los individuos poseen en relación a los datos personales; ya que por las incidencias que día a día en la sociedad se manifiestan, se han perpetrado hechos ilícitos de toda naturaleza que afectan el patrimonio, la libertad y seguridad de los seres humanos.

Los objetivos del presente informe son analizar la problemática derivada de los vacíos que la legislación guatemalteca presenta en relación a la calificación y clasificación de los datos personales que sean de acceso a empresas privadas; la falta de control en relación a los procedimientos y metodologías que establezcan cuales son los datos que se deben proporcionar y el resguardo de los mismos, para evitar que estos sean usados en perjuicio de las personas en futuras ocasiones; y establecer parámetros que regulen y delimiten la información que manejan las empresas privadas, especialmente aquélla que se establezca como confidencial o estrictamente personalísima.

La investigación se enfocó desde un punto de vista jurídico, a efecto de buscar la integración de las leyes; ya que la legislación guatemalteca no posee una normativa que de manera expresa y clara regule la calificación y clasificación de datos personales así como el manejo de las bases de datos y el libre acceso a las empresas privadas, en aras de garantizar los derechos constitucionales en relación a la seguridad jurídica de las personas, así como la protección a la integridad e intimidad de las mismas.

La metodología utilizada fue el método analítico, para comprender los elementos o componentes característicos de la utilización de bases de datos; el sintético para estudiar el manejo y creación de los elementos referidos; el deductivo para conocer las distintas doctrinas que sobre este fenómeno existen en el ámbito jurídico y social; y por último se utilizaron las técnicas bibliográfica y documental que permitieron recopilar y seleccionar adecuadamente el material de estudio.

El presente trabajo se desarrolló en cuatro capítulos, de la siguiente forma: en el primer capítulo se realiza un enfoque general de todo lo relacionado con datos de tipo personal; en el segundo capítulo el desarrollo de los datos personales que sean de acceso a empresas privadas; el tercer capítulo aborda lo referente a conflictos de datos personales en las empresas privadas; y el cuarto capítulo lo relativo a las soluciones planteadas al acceso de datos personales a empresas privadas en Guatemala.

Esperando que este informe sea tomado en cuenta no solamente como material de consulta sino que para que las autoridades de gobierno resguarden y protejan los datos personales e intimidad de las personas; que últimamente se han visto afectadas por la intromisión de empresas privadas que irrespetan el derecho a la privacidad de cada individuo.

CAPÍTULO I

1. Datos personales

La autora Cristina Almuzara establece sobre el tema que: "Son toda información sobre una persona física identificada o identificable, tal como los datos relacionados con su identidad física, fisiológica, psíquica, económica, cultural o social."[1]

Lo anterior expuesto, establece que el alcance de dicha definición implica que los datos personales incluyen, los datos de los registros de población o información provenientes de factores de carácter personal que se pueden verificar o rectificar, cualquier otro elemento, indagación o situación que incluya un contenido de información, con lo que se presume que el conocimiento de una persona individual es identificable.

De este modo, se pueden encontrar datos personales en evaluaciones y juicios subjetivos que, en esa virtud, podrían incluir elementos específicos de la identidad física, fisiológica, psíquica, económica, cultural o social de los interesados, que igualmente sucedería si un juicio o evaluación resultara en una puntuación o clasificación, o si se expresa mediante otros criterios de evaluación.

---

[1] Almuzara Almaida, Cristina. **Estudio práctico sobre la protección de datos de carácter personal.** Pág. 241.

1.1. Aspectos generales de los datos personales

Los principios generales, puede establecerse que definen las pautas que deben, de cierta manera, atenerse a la recolección de datos de carácter personal, como una clase de pautas encaminadas a garantizar tanto la veracidad de la información contenida en los datos almacenados, cuanto la congruencia y la racionalidad de la utilización de los datos.

De lo expuesto, como principio la congruencia y racionalidad, garantizan que los datos no pueden ser usados sino cuando lo justifique la finalidad para la que han sido recabados, así como la característica de observancia, que es capital para evitar la difusión incontrolada de la información que, siguiendo el mandato constitucional se pretende limitar.

Si se toma en cuenta también, el principio de consentimiento o autodeterminación a su vez, los aspectos generales otorgan a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes; la base está constituida por la exigencia del consentimiento consciente e informado del afectado para que la recolección de datos sea lícita; su marco general basa la singularidad de los datos llamados por Emilio Del Peso Navarro como: "Datos sensibles son los que vulneran los sentimientos de las personas y que éstas reservan como un bien propio y susceptible como parte de su mismo ser";[2] refiriendo, que puede ser la propia ideología o creencias religiosas por una parte, cuya privacidad debe estar

[2] Del Peso Navarro, Emilio. **Ley de Protección de Datos: la nueva LORTAD.** Pág. 17.

expresamente garantizada por la Constitución Política de la República de Guatemala, y por otra parte, por ejemplo, la raza, la salud y la vida sexual.

La protección reforzada de los datos personales viene determinada porque los primeros de entre los datos mencionados sólo serán disponibles con el consentimiento expreso y por escrito del afectado; y los segundos, sólo serán susceptibles de recopilación mediando dicho consentimiento o una habilitación legal expresa, habilitación que, según exigencia de la normativa correspondiente, ha de fundamentarse en razones de interés general; también se debe establecer la prohibición de los denominados ficheros, creados con la exclusiva finalidad de almacenar datos personales que expresen las mencionadas características.

Se deben atender los aspectos generales, las exigencias y previsiones que para datos personales, contienen por ejemplo el Convenio Europeo para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal.

1.2. Principios rectores para la calificación y clasificación de datos personales

Se establecen principios que fundamentan los aspectos generales de los datos de identificación personal, que ayudan a regir de mejor manera la información personal; y estos por su parte, definen las pautas a las que debe atenerse la recolección de datos de carácter personal, pautas encaminadas a garantizar tanto

la veracidad de la información contenida en los datos, dentro de los mismos la congruencia y la racionalidad, que garantizan que los datos no puedan ser usados sino cuando lo justifique la finalidad, y su observancia evita la difusión incontrolada, siendo los principios rectores, los siguientes:

Principio de consentimiento

Llamado también de autodeterminación, otorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes, su base está constituida por la exigencia del consentimiento consciente e informado del afectado para que la recopilación de datos sea lícita; su marco, por aparte, se refuerza individualmente en los ya denominados anteriormente datos sensibles.

Principio de finalidad

Para que exista una base de datos, en primer lugar se debe crear un fichero de datos de carácter personal, pero ha de conocerse el fin o utilidad del mismo. Este principio, asimismo, engloba otros dos, que son también de importancia: el principio de pertinencia y el principio de utilización no abusiva.

Principio de pertinencia

Los datos deben ser pertinentes; es decir, estar relacionados con el fin perseguido al crearse el fichero.

La calidad de los datos de carácter personal que se deben recopilar, deberán ser los adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas por las que se hayan obtenido.

Principio de utilización no abusiva

Se infiere de este principio, que los datos recogidos no deben ser utilizados para finalidades incompatibles con aquéllas para las cuales fueron almacenados; asimismo, los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquéllas para las que los datos hubieran sido recolectados, no se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

Principio de exactitud

Quien sea responsable de la creación de ficheros que almacenen datos personales, deberá poner los medios necesarios para comprobar la exactitud de los datos registrados y asegurar su puesta al día; los datos de carácter personal serán exactos y puestos al día de forma que resulten con veracidad a la situación actual del afectado.

Debe atenderse a que si los datos personales registrados resultaran ser inexactos, en todo o en parte; o incompletos, serán cancelados y sustituidos de oficio por los

correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce su tenedor.

Principio de derecho al olvido

Los datos personales deberán desaparecer una vez se haya cumplido con el fin para el que fueron recabados, serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubieren sido almacenados.

Según este principio, reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos; los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

Principio de lealtad

Establece que el procedimiento para recabar los datos a los afectados no ha de ser de forma ilícita o desleal. Asimismo, prohíbe la recolección de datos por medios fraudulentos, desleales o ilícitos.

Hay que establecer con respecto al consentimiento, que presenta una serie de excepciones, dentro de las cuales se puede mencionar que los datos de carácter personal se recojan para el ejercicio de las funciones propias de la administración pública en el ámbito de las competencias; cuando se refieran a las partes de un contrato por ejemplo, o de una relación de negocios, laboral, etc., y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado; y cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Asimismo, hay que tomar en cuenta que en los casos en los cuales no se haga necesario el consentimiento del afectado para el tratamiento de los datos personales, éste se puede oponer a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal.

También, existen principios que rigen la protección de datos, los cuales se analizan a continuación:

1.3. Calidad de los datos

Principio general sobre el que se sustenta la recolección, almacenamiento y tratamiento de los datos de carácter personal. La calidad de los datos son las características que determinan los elementos esenciales que categorizan a los mismos y es por eso que sirven para que se califique a través de un valor social su importancia y privacidad. La calidad de los datos sirve para lograr esta categorización general, que busca la protección de la información personal que pueda ser usada con el propósito de cometer algún delito o dañar la integridad de los seres humanos.

La calidad de los datos se somete a un criterio o juicio de valor socialmente determinado y aceptado que las personas establecen de forma general, es por eso su utilidad como un principio general y básico.

1.4. Información en la recolección de datos

Primera obligación que ha de cumplir el responsable del fichero, si deseare tratar los datos de carácter personal que recaba del afectado. En toda recolección de datos personales que se realice a través de encuestas, estudios de mercado o sondeo de opinión pública u otros instrumentos semejantes, sin perjuicio de los

demás derechos y obligaciones que la ley regula, se deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información. Posteriormente, se establece el procedimiento que determine la forma en que se recolectan los datos y el uso que se le dará a los mismos así como la manera en que se puede acceder a ellos, todo esto sirve para trasparentar la manera en que son recolectados los datos, su forma de almacenamiento y sobre todo los fines para los cuales se recolectan.

1.5. Consentimiento del afectado

Se constituye como un derecho inherente al afectado y; conjuntamente, como deber del responsable del tratamiento. Se da cuando la persona da su consentimiento o permiso para que sus datos personales sean utilizados o registrados en bases de datos, para posteriormente ser utilizados por aquellos requirentes autorizados y con los procedimientos previamente establecidos que garanticen el buen uso de los mismos.

1.6. Datos especialmente protegidos

Se refiere a lo tratado ya anteriormente sobre los datos sensibles, que deben seguir ciertas reglas, a través de las cuales se mantenga la privacidad de la persona. Son especiales porque estos se consideran como un elemento de mayor sensibilidad y que afecta el estado psíquico de las personas, considerados como parte intima de cada ser humano.

1.7. Seguridad de los datos

La persona encargada de la creación de ficheros debe adoptar aquellas medidas técnicas y organizativas acordes a la naturaleza del dato tratado; para ello, cuenta con toda una serie de recursos para la manipulación de los datos que le sean suministrados. Para mantener la seguridad de los datos se deben de tomar las medidas técnicas más idóneas que permitan el archivo, control y mantenimiento de la información, así como los procedimientos para la obtención de los mismos, tomando como primer medida la creación de un marco legal en el cual se encuentre regulada la calificación y calificación de datos personales así como los procedimientos, instituciones, mecanismos técnicos y sanciones en el manejo de la información obtenida. La ley regulara los procedimientos físicos e informáticos que contendrán la información, a través de la creación de archivos electrónicos.

1.8. Transferencia de datos

Es lo que en general se denomina comunicación de datos y la misma se encuentra tasada bajo excepciones o llamados números clausus; asimismo, el traslado de datos lleva aparejada una serie de requisitos formales que siempre han de cumplirse. Entre los requisitos principales serian los datos del requirente, el motivo por el cual necesita de ellos, el uso que dará a los mismos y la confidencialidad y reserva que debe de tenerse de la información. La elaboración de los requisitos y procedimientos para la transferencia de datos estará a cargo de los legisladores y quedara establecido en la ley.

1.9. Acceso a los datos por cuenta de terceros

El acceso consiste en la utilización de los datos personales por empresas distintas a la requirente de la información, con objeto de ser intermediarias o facilitadoras en la obtención de datos, también se puede determinar el acceso por cuenta de terceros como una típica relación entre empresas que prestan servicios al responsable del fichero, es una actividad o una actuación que se verá en la realización de la investigación, ya que el desconocimiento de la misma puede traer respuestas negativas, a pesar de que el resto de principios estuvieren cumplidos.

1.10. Naturaleza de los datos personales

Con respecto a la naturaleza de los datos de carácter personal, se puede atender a varios criterios y teorías que tratan sobre el tema, sin ánimo de extensión sobre el mismo se mencionan algunos autores que establecen diferente posturas sobre la naturaleza de la compilación de datos de información personal.

El autor Abel Téllez indica: "Que la gestión de información personal es, la práctica y el estudio de las actividades que las personas ejecutan a fin de obtener, mantener, recuperar y utilizar piezas de información como documentos de papel y digitales, páginas web y mensajes electrónicos para completar tareas personales o

laborales de la vida cotidiana y cumplir con diversas responsabilidades familiares, laborales, sociales o comunitarias."[3]

De lo anterior se debe tomar en cuenta que, un ideal de la gestión de información personal es que siempre se tenga la información pertinente en el lugar oportuno, en la forma adecuada y con un grado suficiente de calidad para satisfacer la necesidad presente.

La tecnología y las herramientas, como por ejemplo, los asistentes personales, ayudan dedicar menos tiempo a absorbentes actividades de gestión que inducen a cometer errores; así, dejan más tiempo para hacer un uso creativo e inteligente de la información a fin de concluir tareas o simplemente disfrutar de ellas.

Por su parte el autor, Ricardo Martínez y Martínez, indica: "Que una base de datos o banco de datos es un conjunto de datos personales pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido, una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta."[4]

En la actualidad y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital, que ofrece un amplio rango de soluciones al problema de almacenar datos.

---

[3] Téllez Aguilera, Abel. **Criminología.** Pág. 82.
[4] Martínez y Martínez, Ricardo. **La memoria contra el olvido.** Pág. 27.

Existen unos programas denominados sistemas gestores de bases de datos, que permiten almacenar y posteriormente acceder a los datos de forma rápida y estructurada; las propiedades de los mismos, así como la utilización y administración se estudian dentro del ámbito de la informática, las aplicaciones más usuales son para la gestión de empresas e instituciones públicas.

También, son ampliamente utilizadas en entornos científicos con el objeto de almacenar la información experimental, aunque las bases de datos pueden contener muchos tipos de datos, algunos de ellos se encuentran protegidos por las leyes de varios países, por ejemplo en España, los datos personales se encuentran protegidos por la Ley Orgánica de Protección de Datos de Carácter Personal.

Sobre el tema de la naturaleza, Alberto Dalla refiere el hábeas data como: "Una acción legal que tiene la persona que figura en un registro o banco de datos, de acceder a tal registro para conocer qué información existe sobre su persona, y de solicitar la corrección de esa información si le causare algún perjuicio."[5]

Al respecto, este derecho se ha ido expandiendo tanto que comenzó a ser reglamentado por leyes de hábeas data como por normas de protección de datos personales.

[5] Dalla Vía, Alberto R. **La conciencia y el derecho.** Pág. 46.

También se debe hacer mención que, se ha encomendado a organismos de control la vigilancia sobre la aplicación de estas normas; por ejemplo, existen en diversos países como Argentina, Uruguay, España y Francia, temas a tratar en su oportunidad, organismos de control que tienen por misión supervisar el tratamiento de datos personales por parte de empresas e instituciones públicas; también suele exigirse una declaración de los ficheros de carácter personal para generar transparencia sobre su existencia.

El autor antes citado, también indica lo siguiente: "La naturaleza se presenta a través de una información sensible, y es el nombre que recibe la información personal privada de un individuo, por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos."[6]

Aunque lo más común es usar este término para designar datos privados relacionados con internet o la informática, sobre todo contraseñas, tanto de correo electrónico, conexión a internet, identificación personal privada, sesiones del programador, etc., los crackers utilizan la llamada ingeniería social para intentar hacerse con este tipo de información.

Como bien se infiere por el Instituto de Protección de Datos Personales de Madrid, España, con respecto al derecho a la intimidad es que al buen nombre se ha consagrado como un derecho fundamental del ser humano; sin embargo, por

[6] **Ibid**. Pág. 121.

razones de interés público, de orden social y por la concurrencia de otros derechos a la información, no puede considerarse el derecho a la intimidad como un derecho absoluto; por lo tanto, la evolución histórica del hábeas data inicia con un marcado sentido legislativo donde se equilibre la protección de dicho derecho con la libertad de información.

La intelectual Ana Isabel Hernán Ortiz, menciona que : "Atendiendo a la naturaleza de la información deben existir niveles de seguridad o medidas de seguridad, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información."[7]

De esta forma, se establece una atribución de los niveles de seguridad atendiendo a la naturaleza de la información y a su incidencia en los derechos y libertades de las personas, ya que todos los ficheros que contengan datos de carácter personal, deberán adoptar las medidas de seguridad de nivel básico.

Asimismo, los ficheros de datos relativos a la comisión de infracciones administrativas o penales, servicios financieros, y de prestación de servicios de información sobre solvencia patrimonial y crédito; deberán reunir, además de las medidas del nivel básico de seguridad las establecidas a un nivel medio; los ficheros sobre ideología, religiosos, creencias, origen racial, salud o vida sexual; o los que tengan información recabada con fines policiales sin consentimiento de los

[7] Hernán Ortiz, Ana Isabel. **El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales.** Pág. 45.

interesados, deberán reunir además las medidas de seguridad correspondientes al más alto nivel.

Por último, los ficheros que contengan datos personales suficientes que permitan obtener una evaluación de la personalidad del individuo; deberán garantizar además, suficiente seguridad y confidencialidad. Estas medidas a su vez deben reforzar a medida de la peligrosidad y riesgo de datos, no tratar de establecer en cada caso medidas diferentes, sino de reforzar y establecer mayores controles para las ya previstas en cada caso.

1.11. Clasificación y calificación de los datos personales

Para poder establecer la clasificación y calificación de los datos personales, hay que definir lo que es una base de datos y los aspectos que enmarca la calificación del mismo, para poder llegar de lo general a lo específico y se infiere en lo siguiente:

1.11.1 Base de datos

Como menciona en su tesis el autor Rodrigo Cano: "Una base o banco de datos es un conjunto de hechos, datos y otra información armada en un formato

organizado susceptible de utilizarse mediante computación comprendiendo uno o más documentos."[8]

Las bases de datos son definidas como un conjunto de colecciones de datos; es decir, de ficheros conexos o relacionados; a continuación se menciona su calificación.

El minado de datos

Llamado por su siglas en inglés data mining, consiste en una técnica para obtener datos relevantes entre gran cantidad de información almacenada con anterioridad en bases de datos; hay que mencionar que el aumento de la capacidad de almacenamiento y procesamiento de grandes volúmenes de información sistematizada, aumenta también la necesidad de extraer patrones entre todo ese cúmulo de información recabada.

Esta técnica analiza la información con el objeto final de facilitar el acceso a los datos, utilizando en la mayoría de casos sistemas basados en un sistema operativo inteligente.

[8] Cano Morales, Rodrigo. **Acción de habeas data como mecanismo de la protección jurídica de los datos personales.** Pág. 8.

El almacén de datos

Esta técnica, llamada en inglés data warehouse, tiene como principal presupuesto recolectar y agrupar los datos con el propósito de facilitar su posterior análisis, de manera que sea útil para acceder y analizar la información recabada a través del data mining.

Tiende a ser un proceso a través del cual las bases de datos de una empresa por ejemplo, utilizan los ordenadores como medio para organizar la información obtenida, de manera que sea comprensible para las personas que la utilicen, lo cual es esencial para cualquier institución, ya que constituye un elemento principal en cualquier circunstancia.

Por otra parte, se debe atender a la clasificación de las bases de datos, las cuales se deben agrupar en dos grupos muy importantes, las bases de datos de carácter público y bases de datos de carácter privado.

Bases de datos de carácter público

Se utiliza el término público, ya que son públicos los registros que tiene el Estado para el almacenamiento de datos relativos a una actividad, que por seguridad jurídica se debe mantener en custodia y con un respaldo documental, el cual puede transferirse y por lo general es información que está disponible para cualquier persona sin requisito alguno.

El Artículo 31 de la Constitución Política de la República de Guatemala, en su parte conducente establece: "Acceso a archivos y registros estatales. Toda persona tiene 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."

Bases de datos de carácter privado

Privados son los archivos que se conservan por personas físicas o jurídicas con una finalidad determinada y de particular naturaleza. Si se utilizan para una simple información personal no afectan la intimidad mientras no se logre identificar a persona alguna en particular; en cuyo caso, el afectado o titular de la información podría requerir el acceso a la base de datos y solicitar explicaciones sobre la finalidad del registro.

1.11.2. Clasificación de los datos personales

Por su parte el autor Oscar Raúl Puccinelli, expone la siguiente definición: "El vocablo dato se refiere a un elemento circunscrito y aislado, que no alcanza a tener el carácter de información, pues para que se transforme en ella se requiere la interconexión de esos datos de manera que, vinculados, se conviertan en una referencia concreta."[9]

[9] Puccinelli, Oscar Raúl. **El habeas data en el constitucionalismo indo iberoamericano finisecular, en el amparo constitucional.** Pág. 95.

Haciendo alusión al concepto, para poder entender la clasificación de los datos personales propiamente; es importante indicar que la información personal que registran los archivos ya sean éstos de carácter privado o público, proviene de dos fuentes principales, las fuentes directas que consisten en aquellos datos voluntariamente prestados por su titular y, fuentes indirectas, aquellos datos que se obtienen de otras bases de datos, siendo que la interconexión de las mismas y transferencia de datos determinan el origen o lugar de procedencia de la información.

También se puede mencionar que la teoría relacionada con la informática clasifica en una gran variedad de categorías los datos personales, pero la clasificación más sencilla y completa es la que refiere el autor Gozaíni: "Por la identificación del titular del dato y por la confidencialidad de la información."[10]

Dicha clasificación se define a continuación y ayudará a entender y reconocer la importancia y objeto de proteger los datos personales como garantía constitucional.

Por la identificación del titular del dato

a) Nominativo: que es el dato de una persona física o jurídica conocida e identificada;

[10] Gozaíni, Osvaldo Alfredo. **Habeas data, protección de datos personales, doctrina y jurisprudencia.** Pág. 231.

b) Innominativo o anónimo: que es el dato de uso estadístico o científico que no identifica a persona alguna, porque la información archivada no se refiere a él o a ella, sino a sus actividades.

Por la confidencialidad de la información

a) Datos que no afectan la sensibilidad de las personas: se trata de aquella información irrelevante que por las características que tiene no permite herir los sentimientos más íntimos de la persona ni afecta su derecho a la privacidad. Es el dato rutinario, el que se ofrece sin complicaciones o se obtiene de fuentes fácilmente accesibles.

b) Datos que afectan la sensibilidad de las personas: son los que de difundirse ponen en conocimiento de quien los conoce datos de contenido privado que salvo manifestación expresa del afectado, socavan la intimidad de las personas.

Por la subjetividad o pertenencia del dato

a) Datos personales existenciales: se denomina así a los datos que se relacionan con definidores de la personalidad, tales como el lugar de origen, estado civil, domicilio, profesión, entre otros.

b) Datos personales no existenciales: aquéllos vinculados con el patrimonio económico y con la pertenencia de cosas que identifican.

Por el secreto que guardan

a) Datos personales secretos y/o confidenciales: datos que conservan una categoría propia, observada en relación con alguien que debe preservar el deber de ocultación de los mismos. En esta materia, el tratamiento de datos obliga a conservar el secreto a quienes hayan trabajado en las bases de datos; y por ello, tomado conocimiento de la información personal archivada.

b) Datos sensibles: en términos generales, ya mencionados anteriormente, pertenecen a una categoría única que atiende esencialmente al derecho a la privacidad personal; son informaciones que afectan la esfera máxima de intimidad y que merecen un tratamiento particular.

1.12. Procedimiento para el procesamiento en la clasificación y calificación de datos personales

A partir de la formación de un archivo, los datos personales que se recopilan, son sometidos a una serie de etapas y procedimientos distintos que van generando una serie de consecuencias jurídicas, algunas sin mayor repercusión y otras operaciones más complejas.

Cada fase o etapa tiene repercusión particular que incide por el carácter sinalagmático, tanto en los derechos como en las obligaciones de quienes participan o intervienen en el tratamiento de los datos de carácter personal; las etapas o fases que tienen en su proceso operacional, son las siguientes:

Etapa de búsqueda, localización y almacenamiento del dato

Antes de llegar al archivo de datos personales, es preciso obtenerlos, para lo cual se hace necesario buscarlos o localizarlos; y una vez ubicados, debe procurarse que el individuo que aporta al información otorgue su consentimiento para incorporarlos a un banco de datos; o en su caso, si la búsqueda y localización se realiza de manera indirecta, el consentimiento se debe lograr, tanto del lugar del cual se obtiene como del titular concernido o afectado.

Etapa de clasificación, procesamiento y seguridad del dato

Después de haber realizado la recolección oportuna del dato, se debe proseguir al tratamiento de los datos personales, que son las operaciones y procedimientos técnicos de carácter automatizado o no, que permiten la obtención, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

A criterio de muchos doctrinarios en la materia, esta etapa representa la fase más conflictiva y la que tiene dimensiones distintas, según la naturaleza del procedimiento de los datos que se haga por fuentes habituales como lo son la organización y clasificación del registro, o se realice por entrecruzamiento o interconexión y que son operaciones que abarcan la vinculación de más de un archivo.

Etapa de interconexión o adquisición de datos

También denominada etapa de entrecruzamiento de datos, consiste en una fase meramente técnica que produce la interrelación entre bancos de datos para lograr un perfil mejorado de la información.

Etapa de cesión parcial o total, local o internacional de datos

La cesión de los datos, constituye la etapa final del proceso; participan en ella el sujeto titular de los datos, las personas que tratan la información y el responsable del archivo, el cesionario o adquirente y los organismos que controlan la transmisión de manera directa o indirecta.

De acuerdo al autor Gozaíni, se utilizan los siguientes términos: "Transmision local, si la misma se realiza en el territorio nacional, o transmisión internacional de

datos o flujos internacionales de datos para expresar el intercambio de información en el ámbito internacional."[11]

1.13. Importancia de la calificación de la base de datos

Tomando en cuenta el epígrafe de un movimiento internacional de datos, se toma en cuenta la regulación de la transmisión internacional de las informaciones de carácter personal, esta regulación a la que se debe hacer referencia está en sintonía con la regulación del flujo transfronterizo de datos, ya que la finalidad debe ser conciliar la protección de la integridad de la información personal, con el libre tránsito de los datos.

Se tiene que hacer mención de ese tránsito, pues la transmisión internacional de datos, constituye una auténtica necesidad de la vida actual y de suma importancia en el ámbito económico del Estado, tal y como evidencia la gran cantidad de inversiones que en los últimos años se han venido manifestando, como bien lo menciona el autor Madec: "En relación con el entorno de la libre circulación de informaciones y de datos, es un marco necesario para su funcionamiento."[12]

De aquí se deduce que la importancia de la transmisión de datos personales es tal para la economía de un país, que para este autor, cualquier restricción repentina

[11] Gozaíni. **Ob. Cit.** Pág. 225.
[12] Madec, A. **El mercado internacional de la información, los flujos transfronteras de información y datos.** Pág. 84.

a este flujo sería similar a los de un bloqueo o un embargo, o un acto de guerra económica.

La importancia en el manejo de datos personales radica en tomar en cuenta la norma general en la transmisión internacional de datos, que es la de exigir un sistema de protección equiparable para los datos que se utilizan y la forma en que se manipulan, cuyo sentido último lo infieren los autores Piñol y Estadella así : "Es lograr compatibilizar el principio de libre circulación de la información con el principio de defensa del derecho humano a la intimidad de los particulares sobre sus datos."[13]

Es decir que, este principio responde, por una parte, a las necesidades de garantizar una protección semejante en la transmisión de datos personales, a las de la comunicación y a las exigencias de los convenios y tratados referentes al tema.

Se deduce también que la protección de datos personales debe exigir, para su transmisión, un cierto nivel de protección adecuada, esta manipulación en la transmisión se adecúa en muchos casos a criterios diferentes, o sea a un posible nivel de protección. El nivel de protección obedece a la categorización que se realiza derivado del análisis e importancia, aportando los elementos que hacen

[13] Piñol Rull, Osman y Oscar Estadella Yuste. **La regulación de la transmisión internacional de datos.** Pág. 85.

posible el encuadramiento de la información que se pretende clasificar y otorgarle así el nivel de protección a los datos.

1.14. Reseña histórica de los datos personales

Se debe iniciar teniendo en cuenta la intimidad de la persona, el respeto y la intimidad del ser humano; el derecho moderno no hace otra cosa que redescubrir un valor tradicional, que era conocido desde la edad media, pero como derecho a la vida surge de manera específica en los Estados Unidos de América en 1890, planteado por dos abogados de Boston, Samuel Warren y Louis Brandéis que publicaron en el Harvard Law Review, el libro titulado: The Right Of Privacy; pero ya, el juez norteamericano Cooley, había proclamado el derecho de ser dejado tranquilo y de no ser arrastrado por la publicidad, como lo propio del derecho a la intimidad.

Por otro lado, hasta antes de la vigencia de la ley del 17 de julio de 1970, que tiene una parte destinada a la protección de la vida privada; la doctrina y la jurisprudencia de Francia habían adelantado bastante en la creación jurídica del concepto. Juristas franceses elaboraron primero la noción de los derechos de la personalidad, para que luego los tribunales impusieran su respeto por la vía de la aplicación del Artículo 1382 del Código Civil francés, sobre la responsabilidad extracontractual, esto debido a que la jurisprudencia se fue unificando, principalmente a reclamos de artistas y gentes del mundo.

En cambio, las legislaciones hispanoamericanas, no hacen referencia directa al derecho del respeto a la vida privada, aún así, se presta amparo a varios importantes aspectos de que derecho se priva, existiendo reglas jurídicas relativas a la protección del domicilio, el secreto de la correspondencia y en la actualidad el acceso de información por medios electrónicos.

El Artículo 12 de la Declaración Universal de los Derechos Humanos de 1948, estatuye que: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques; siendo ésta la primera referencia oficial a la protección a la vida privada.

El inciso primero del Artículo 8 de la Convención Europea de los Derechos Humanos de 1950 indica que: "Toda persona tiene derecho al respeto a la vida privada y familiar, de su domicilio y de su correspondencia; asimismo, los incisos dos y tres del Artículo 11 de la Convención Americana de Derechos Humanos de 1969 en San José, se refieren también al derecho a la vida privada.

En la vida de una sociedad moderna y tecnificada, el derecho a la vida privada, se ha transformado en una materia que ha de analizarse con mucha dedicación, en virtud que se advierten varias amenazas en contra del respeto a la intimidad. Asimismo, se debe tomar en cuenta el gran desarrollo de los medios masivos de comunicación, así como medios electrónicos, que lleva muchas veces a personas

malintencionadas, a tratar de satisfacer la curiosidad de un público ávido, amplio y heterogéneo, como es el ejemplo de los periodistas, que necesitan de información muchas veces de personajes relevantes de la vida política, publica, etc., con el fin de comercializar ésta a través de los medios correspondientes.

Como menciona el autor Azofeifa: "En su formulación inicial, de raigambre anglosajona, el derecho a la privacidad, es un derecho moderno que aparece al compás del desarrollo de las primeras manifestaciones de los massmedia o medios de comunicación en masa, esto es, de las formas de intrusión en la esfera personal, cuando la presión social sobre la esfera privada se patentiza."[14]

De lo anterior citado, se deduce a su vez que la evolución del derecho a la intimidad, inicia del concepto liberal de la propiedad, en tanto que dicho derecho no constriña a no ser afectado en el goce y disfrute de la cosa poseída.

Posteriormente, al menos a partir de 1890, el interés se traslada al resguardo de la privacidad ante la amenaza de fotógrafos, periodistas, entre otros; y el derecho a la intimidad encontrará aportes jurisprudenciales y legislativos hasta el presente siglo.

Hasta finales de los años sesenta, tanto en los Estados Unidos de América como en Europa, es que el derecho a la intimidad puede ser observado como una

[14] Azofeifa. **Ob. Cit.** Pág. 37.

categoría jurídica independiente, esta categorización surge con los primeros años del Estado intervencionista y su reacción contra el antiguo sistema liberal.

El Estado intervencionista o de derecho social tenía objetivos de control muy concretos que agregarían contradicciones de las primeras manifestaciones legislativas y constitucionales del derecho a la intimidad; mientras que en el Estado liberal la conciencia individual se consideraba como algo sin relevancia para los fines públicos, ya que el individuo tenia plenas libertades de acción y pensamiento en lo particular, siempre y cuando no perjudicara el derecho de los demás.

Se debe hacer mención de los antecedentes del hábeas data, en virtud que es de suma importancia su aplicabilidad y desarrollo, tal como se analizará en su oportunidad en la presente investigación.

1.15. Antecedentes del hábeas data

En la década de los años 70 del siglo XX, diversos países europeos fueron elaborando legislación destinada específicamente a la protección de datos frente al avance informático; inicialmente Alemania, Dinamarca, Francia, Luxemburgo, Noruega, Reino Unido y Suecia, entre otros, regularon el derecho de acceso a la información personal y el derecho de rectificación de los datos inexactos, obsoletos, discriminatorios o ilícitamente colectados.

En el seno del Consejo de Europa en 1967, se constituyó una comisión consultiva para estudiar las tecnologías de la información y su potencial agresividad hacia los derechos de la persona; de esos estudios proviene la Resolución 509 de 1968, de la Asamblea del Consejo de Europa, sobre derechos humanos y los nuevos logros científicos y técnicos, cuyos principios versaban sobre la necesidad de que las informaciones obtenidas fueran legales, exactas, actualizadas y apropiadas al fin para el cual fueran almacenadas.

Asimismo, se reconoció el derecho de todo ciudadano a conocer la información acumulada sobre su persona y la obligación de aquellas instituciones o empresas que operaban bases de datos, a conducirse bajo normas estrictas, a efecto de garantizar el mantenimiento del secreto y prevenir el mal uso de los datos.

Tiempo después, se promulgó el Convenio Europeo de Protección de Datos del 28 de enero de 1981, firmado en Estrasburgo, con la finalidad de garantizar en el territorio de los Estados parte, a cualquier persona física, el derecho a la vida privada con respecto al tratamiento automatizado de los datos de carácter personal.

Si bien fue asumida en el plano de la legislación ordinaria, no fue ajena a la preocupación de los constituyentes europeos, la problemática del proceso de protección de datos; las primeras constituciones que abordan el problema generado por la aparición de la informática sobre los derechos fundamentales de las personas, fueron las de Portugal de 1976 en la cual el Artículo 35 establece:

"1. Todos los ciudadanos tienen derecho a tomar conocimiento de los datos constantes en ficheros o registros informáticos a su respecto y del fin a que se destinan, pudiendo exigir su rectificación y actualización, sin perjuicio de lo dispuesto en la Ley sobre Secretos de Estado y Secretos de Justicia. 2. Es prohibido el acceso a ficheros y registros informáticos para conocimiento de datos personales relativos a terceros y su respectiva interconexión, salvo en casos excepcionales de ley. 3. La informática no puede ser utilizada para el tratamiento de datos referentes a convicciones fisiológicas o políticas, filiación partidaria o sindical, fe religiosa o vida privada, salvo cuando se trate de procesamiento de datos estadísticos individualmente identificables."

Posteriormente le siguió la legislación de España en 1978, luego Gran Bretaña sancionó la Ley de Hábeas Data en 1984, en tanto que en los Estados Unidos de América ello ocurrió en 1974, con el nombre de Ley sobre Privacidad conocida como Freedom of Information Act. Dicha legislación aporta todo un sistema sobre libertad de información y su respectivo trámite administrativo; este régimen instaló una fuente de acción pública a la información, afirmando el derecho del pueblo a obtenerla de los registros existentes en la administración pública, salvo que estuvieren clasificados como secretos.

Uno de los elementos más importantes y característicos de la ley norteamericana sobre privacidad de 1974, es la de establecer una prohibición de bancos de datos secretos en materia de información personal; el derecho de todos los habitantes de conocer información que le concierne, y que está depositada en los bancos, así

como saber cuál va ser el uso que se hará de ella; el derecho de cada interesado de corregir o ratificar la información registrada que a él le concierna; la prohibición para el registro de utilizar información personal, sin permiso del interesado, para otro propósito diferente para el cual dispuso la autorización respectiva.

Del otro lado del continente, en España, la Constitución Política contiene una amplia protección de los derechos a la información, al uso de la información, así como en general a la libre circulación de las ideas.

En España la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), que entró en vigencia el 14 de enero de 2000, reglamenta a su vez el Artículo 18 numeral cuarto de la Constitución Política española: "Garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar."

Es decir, que el legislador prevé el uso de la informática para garantizar el honor y la intimidad personal, o familiar de los ciudadanos, estableciendo esto uno de los objetivos de dicha normativa.

En Alemania, la institucionalización del hábeas data ocurre en 1977 con la promulgación de la Ley Federal para la Protección Contra el Uso Ilícito de Datos Personales; que tiene carácter de aplicación general a todo tipo de registros, sean éstos automáticos o manuales, públicos o privados, siempre que en ellos se

procesen datos personales, estableciendo como requisito primordial, el consentimiento del interesado previo al registro del dato, y la obligación de los titulares de los archivos o bancos de datos de comunicar este hecho a los ciudadanos.

Francia a su vez, promulga en 1987, la Ley de Protección a los Datos e Información Informática, con el propósito de crear la Comisión Nacional de Informática y de Libertades, que tiene en la actualidad como finalidad regular el funcionamiento de la informática, la organización de sus registros y de establecer las libertades y derechos que genera el sistema, definiendo la forma en que deben desarrollarse las relaciones entre la administración pública y la sociedad en relación a la información de los datos personales.

De este lado del continente, una de las primeras constituciones latinoamericanas que introdujo a su tenor, regulando el hábeas data como una garantía específica fue Brasil, la cual establece en el Artículo 5 inciso LXXI de la Ley Fundamental que: "Se concederá hábeas data: a) para asegurar el conocimiento de informaciones relativas a la persona que consten en registros o bancos de datos de entidades gubernamentales o de carácter público, b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo."

De lo anterior citado, comenta el autor Gozaini que: "Cuando ella prevé como efecto del hábeas data la rectificación de los datos importa también la

actualización, corrección y hasta la supresión de los mismos cuando ellos fueron incorrectos."[15]

Asimismo, en el apartado de la misma normativa, el Artículo 5 constitucional consagra la acción popular a favor de cualquier ciudadano para interponer hábeas data que tenga por objeto anular un acto lesivo al patrimonio público o de una entidad donde participe el Estado, cuando estuviere afectada la moralidad administrativa, el medio ambiente o el patrimonio histórico y cultural.

Por su parte, la Constitución Política colombiana de 1991, asume la problemática relativa al tratamiento de datos, incorporando a la legislación normas relativas al manejo de información personal; es así que, en el Artículo 15 estatuye: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerse 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."

También, la Constitución Política de Paraguay de 1992, incorpora a su texto la previsión de que toda persona puede 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 de conocer el uso que se haga de los mismos y de su finalidad, también podrá la persona solicitar ante el magistrado competente la

[15] Gozaíni. **Ob. Cit.** Pág. 259.

actualización, rectificación o la destrucción de aquéllos, si fuesen erróneos o afectaran ilegítimamente sus derechos.

La Constitución Política de Perú de 1993, se convierte en la primera en abordar el tema de una forma más amplia e integral, inspirándose en los antecedentes brasileños y perfilando al hábeas data como una acción; definiendo el contenido del derecho a la protección de los datos personales.

En Argentina en 1994, el hábeas data es elevado a rango constitucional, así el tercer párrafo del Artículo 43 de la Constitución Nacional de Argentina establece que: "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística."

Aunque no adopta expresamente ese nombre hasta con la promulgación de la Ley 25.326 que reglamenta propiamente el hábeas data.

Ecuador, reforma su Constitución Nacional en 1998 e incluye en el cuerpo legislativo que: "Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes consten en entidades públicas o privadas, así como conocer el uso que se haga de ellos y su

propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar la indemnización."

Esta ley establece un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional.

Todo lo anterior expuesto constituye dentro del análisis de los datos personales, los aspectos más importantes así como un repaso general de los antecedentes de mayor impacto en la formación del hábeas data y su institucionalización. Además de la legislación expuesta existen otros países que no cuentan con esta garantía constitucional, pero se ha procedido a encontrar una forma de defensa, desarrollando proyectos que impulsen la defensa sobre datos de carácter personal.


FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Guatemala, C. A.

CAPÍTULO II

2. Desarrollo de los datos personales que sean de acceso a empresas privadas en Guatemala

Es de hacer notar que la utilización y manejo en la captación de datos de carácter personal, es de suma importancia para la privacidad y el respeto de los mismos; así también, la creación de ficheros compilados exige un grado técnico de profesionalismo, compromiso y acatamiento para la integridad personal y la información que se consigne dentro de ellos.

2.1. Desarrollo de la calificación y clasificación de datos personales

En este tema surgen muchas interrogantes jurídicas, pero como principal punto el derecho aplicable, la jurisdicción, la protección de la vida privada del consumidor y la protección de los datos, siguen sin resolverse a cualquier nivel tanto nacional como internacionalmente; aún así países en desarrollo han logrado cierto grado de previsibilidad y seguridad jurídica, sancionando legislación que reconoce el valor jurídico y legal de los medios electrónicos de comunicación de manejo de datos personales.

Por ejemplo, algunos países en desarrollo ya han aprobado leyes basadas en la Ley Modelo sobre Comercio Electrónico de 1996 de la Comisión de las Naciones Unidas para el Desarrollo Mercantil Internacional, cuyo objetivo principal es ofrecer

a los legisladores un conjunto de normas internacionalmente aceptables que permitan eliminar algunos obstáculos jurídicos y crear un marco legal más seguro para el manejo de ficheros de información electrónica.

Como se ha mencionado, la seguridad es otro campo en el cual se ha hecho muy poco, ya que por ejemplo la falta de un marco jurídico adecuado sobre la seguridad de la información y la infraestructura y el delito cibernético, impide a los países en desarrollo aprovechar las oportunidades que ofrece el comercio y el trato de información personal electrónica.

Sobre la protección de los datos y el secreto de la información, son pocos los países que han tratado el tema sobre normativas que regulen la reunión, el uso, la difusión y la protección de los datos personales a que tienen acceso las empresas por internet.

La falta de regulación en este campo es evidentemente perjudicial para la economía nacional de numerosos países en desarrollo; pero para evitar que se eluda la ley pasando por otros medios y para proteger los derechos de las personas sobre sus datos personales, prohíben la transferencia de datos personales a países en que los datos no tienen un grado parecido o suficiente de protección; para evitar las consecuencias negativas de tales restricciones, los países en desarrollo tienen que normar protección de datos.

2.2. Fuentes de manejo y captación de datos personales por parte de las empresas privadas en Guatemala

La mayoría de tratos abusivos en el manejo de datos personales, como ficheros electrónicos de información, o los llamados burós electrónicos, son dirigidos en su tratamiento a servicios web en su mayoría, que se refiere a la interacción automatizada por internet entre computadoras que manejan diferentes procesos empresariales, crean redes de información entre computadoras en las que cada una produce información y viceversa.

Tal manejo de información entre sistemas operativos se realiza a través de software diseñado para usar otro software, llegando así a la comunicación entre ambos; los servicios web tienen el potencial para elevar considerablemente la eficiencia de procesos automatizados de información, así como un control existente de datos personales.

Por otro lado, los servicios web que manejan las empresas también pueden ser muy útiles para integrar sistemas diferentes, como los de la cadena de suministros basados en el intercambio electrónico de datos o el lenguaje extensible de marcado.

El uso de dichos servicios seguramente se extenderá a otros procesos empresariales, porque hacen posible la interoperabilidad automática e

ininterrumpida entre las aplicaciones usadas para manejar los diversos aspectos de una empresa, así como con las aplicaciones de clientes y proveedores.

De cierta manera, se debe entender que estos servicios serán parte esencial de una economía en que la comunicación entre objetos basados en internet será cada vez más importante; éstos afectarán principalmente a las operaciones de las empresas, pero también hay posibilidades para la aplicación orientada a los derechos del consumidor, y el manejo de su información personal, para actividades propias de una empresa.

Los servicios web tienen el potencial de convertirse en un factor de cambio importante ya que están en la confluencia de varias formas de trato de datos, que cambian a su vez la organización e interacción de las mismas y podrían influir en el futuro de la comunicación e información de datos.

Como primera tendencia hay que enmarcar la influencia del manejo y desarrollo de los servicios, la integración de las cadenas de transición en gestión de demanda de información personal, que puede afectar en un futuro próximo un trato de la persona afectada hacia el mal uso de su propia información.

Como lo expresa la Secretaría de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD): "Hay continuidad también en la desigualdad de la inclusión de los países en desarrollo en la información digital, hoy en día es evidente que los gobiernos, la sociedad civil y las empresas de un número

alentador de países en desarrollo han entendido la importancia de las cuestiones en juego y trabajan para ayudar a la protección de datos de una población sin ningún carácter de discriminación."[16]

Con ese objeto, es necesario entender los mecanismos para la captación de información electrónico que sean de carácter personal.

2.3. Controles de la información de datos personales

Se inicia haciendo referencia que para el manejo de datos de información de carácter personal, se atiende a criterios en su tratamiento y recopilación, que sirvan de marco de seguridad para el uso y difusión de información personal electrónica, que pueda afectar a una persona; el autor Álvaro Sánchez menciona que dichas medidas pueden agruparse atendiendo a cuatro criterios fundamentales:

a. "Controles personales: Para el tratamiento de datos personales sólo podrá designarse a personas especialmente cualificadas y que estén sometidas a controles de seguridad. Estas personas autorizadas sólo deben disponer de acceso a los datos que sean de su competencia. Estas medidas tienden a impedir que los sistemas de tratamiento de datos puedan ser utilizados por personas no autorizadas haciendo uso de las instalaciones de transmisión de datos.

[16] UNCTAD. **Informe sobre comercio electrónico y desarrollo 2003.** Pág. 37.

b. Control de instalaciones: Deben adoptarse medidas para impedir que personas no autorizadas accedan a las instalaciones utilizadas para la transmisión de datos.

c. Controles en el tratamiento: Las medidas deben tender a impedir la introducción, información, comunicación o retirada de datos sin autorización.

d. Controles en la transmisión: Tendrá que impedirse que los datos sean leídos, copiados, modificados o suprimidos sin autorización durante la transmisión de los datos."[17]

Según la anterior cita, se pretende con ello salvaguardar la integridad de los soportes de datos, y evitar que cualquier persona no autorizada, una vez que haya accedido a las instalaciones las pueda leer, copiar, modificar o retirar los soportes de datos; asimismo, debe poderse comprobar y verificar que el tratamiento de datos hayan sido introducidos, por qué personas y en qué momentos.

2.4. Legislación existente que regula la protección de los datos personales

Como antecedente la norma superior en Guatemala, la Constitución Política de la República de Guatemala preceptúa protección a las acciones privadas, al principio

[17] Sánchez Bravo, Álvaro A. **La protección del derecho a la libertad informática en la Unión Europea.** Pág. 197.

de reserva y reconoce, la actuación privada del ser humano en su domicilio particular; así también, la información contenida en su correspondencia y en conversaciones telefónicas de carácter privado no deben ser objeto de publicidad, a menos que la persona decida lo contrario; asimismo, regula el respeto e igualdad de las personas.

Se estatuye en el Artículo 23, la inviolabilidad de la vivienda y menciona que: "La vivienda es inviolable. Nadie podrá penetrar en morada ajena sin permiso de quien la habita, salvo por orden escrita de juez competente en la que se especifique el motivo de la diligencia y nunca antes de las seis ni después de las dieciocho horas. Tal diligencia se realizará en presencia del interesado, o de su mandatario."

Es así, que tanto la inviolabilidad de datos dentro de la vivienda también está protegida por la Carta Magna, ya que los datos personales forman parte de la integridad, y si son mal usados se viola la misma.

El Artículo 24 por su parte establece: "Inviolabilidad de correspondencia, documentos y libros. La correspondencia de toda persona, sus documentos y libros son inviolables. Sólo podrán revisarse o incautarse, en virtud de resolución firme dictada por juez competente y con las formalidades legales. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna. Los libros, documentos y archivos que se relacionan con el pago de impuestos, tasas, arbitrios y contribuciones, podrán ser revisados por la autoridad competente de conformidad

con la ley. Es punible revelar el monto de los impuestos pagados, utilidades, pérdidas, costos y cualquier otro daño referente a las contabilidades revisadas a personas individuales o jurídicas con excepción de los balances generales, cuya publicación ordene la ley. Los documentos o informaciones obtenidas con violación de este artículo no producen fe ni hacen prueba en juicio."

Del articulado citado, se puede deducir que todo lo preceptuado es en la actualidad digitalizado, para la supuesta rapidez en la diligencia de la información, pero que en muchos casos, se dilata y abusa de la misma, dejando al descubierto la información personal tergiversada con intenciones ilícitas, que viola este derecho a la protección de los datos.

Asimismo el Artículo 31 preceptúa: "Acceso a archivos y registros estatales: Toda persona tiene 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 corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos."

De lo anterior se infiere que, tanto el manejo de archivos de información tienen un derecho y una prohibición; para lo cual, también debe referirse que en la era moderna ya existe digitalización de esta forma de información, pero imaginemos su mal uso, por ejemplo de archivos de personas del mundo político, podrían

violarse sus derechos o más aún, con la utilización de esta información por empresas se puede dar la discriminación hacia otras personas.

Por otro lado el Código Civil de Guatemala instituye en el Artículo 1656: "Difamación. En caso de difamación, calumnia o injuria, la reparación se determinará al daño moral y a los perjuicios que se deriven."

Como bien lo menciona el autor Rodrigo Cano, respecto al tema: "Tanto en el Código Civil como en el Código Penal guatemalteco, el legislador lo tuvo en cuenta y lo sancionó, tanto civil como penalmente en la medida que constituye una amenaza al honor de las personas y consecuentemente al derecho a su intimidad."[18]

De lo antes citado, el Código Penal a su vez estatuye en el Artículo 161: "Injuria. Es injuria toda expresión o acción ejecutada en deshonra, descrédito o menosprecio de otra persona. El responsable de injuria será sancionado con prisión de dos meses a un año."

El Artículo 164 del mismo Código estipula que: "Difamación. Hay delito de difamación cuando las imputaciones constitutivas de calumnia o injuria se hicieren en forma o por medios de divulgación que puedan provocar odio o descrédito, o que menoscaben el honor, la dignidad o el decoro del ofendido, ante la sociedad. Al responsable de difamación se le sancionará con prisión de dos a cinco años."

[18] Cano Morales, Rodrigo. **Ob. Cit.** Pág. 22

El Artículo 217 indica: "Violación de correspondencia y papeles privados. Quien, de propósito o para descubrir los secretos de otro, abriere correspondencia, pliego cerrado o despachos telegráficos, telefónicos o de otra naturaleza, que no le estén dirigidos o quien sin abrirlos, se impusiere de su contenido será sancionado con multa de cien a mil quetzales."

Artículo 218: "Sustracción, desvío o supresión de correspondencia. Quien, indebidamente, se apoderare de correspondencia, pliego o despachos, a que se refiere el Artículo anterior o de otro papel privado, aunque no estén cerrados o quien los suprimiere o desviare de su destino, será sancionado con multa de cien a mil quetzales."

El Artículo 222 establece: "Publicidad indebida. Quien hallándose legítimamente en posesión de correspondencia, de papeles o de grabaciones, fotografías no destinadas a la publicidad los hiciere públicos, sin la debida autorización, aunque le hubieren sido dirigidos cuando el hecho cause o pudiere causar perjuicio, será sancionado con multa de doscientos a dos mil quetzales."

El Artículo 223 norma: "Revelación de secreto profesional. Quien sin justa causa, revelare o empleare en provecho propio o ajeno un secreto del que se ha enterado por razón de su estado, oficio, empleo, profesión o arte, si con ello ocasionare o pudiere ocasionar perjuicio, será sancionado con prisión de seis meses a dos años y de cien a un mil quetzales de multa."

Asimismo el Artículo 274 inciso D) refiere: "Registros prohibidos. Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que pueden afectar la intimidad de las personas."

En los Artículos antes citados, se preceptúa y protege tanto la violación de privacidad como la creación de bases electrónicas de datos y su mala utilización; pero hay que tomar en cuenta que existen otras normas que regulan la protección de tales aspectos, como las siguientes:

La Convención Americana sobre Derechos Humanos en el Artículo 11 establece la protección de la honra y dignidad y establece que: "Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. Nadie puede ser objeto de injerencias arbitrarias o abusivas con su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra y reputación. Toda persona tienen derecho a la protección de la ley contra esas injerencias o esos ataques."

Asimismo, la Declaración Universal de los Derechos Humanos, en el Artículo 12 estatuye: "Nadie puede ser 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."

La Declaración Americana de los Derechos y Deberes del Hombre, preceptúa en el Artículo 5: "Derecho a la protección, a la honra, la reputación personal y la vida privada y familiar. 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."

El Artículo 9 del mismo normativo establece: "Derecho a la inviolabilidad del domicilio. Toda persona tiene el derecho a la inviolabilidad de su domicilio; y el Artículo 10: "Derecho a la inviolabilidad y circulación de la correspondencia. Toda persona tiene el derecho a la inviolabilidad y circulación de su correspondencia."

Del tema se desprende a su vez, el Pacto Internacional de Derechos Civiles y Políticos, Artículo 17: "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."

2.5. Reserva legal de datos personales

Como principio, la reserva legal de información de carácter personal determina que es necesaria una norma con rango legal para habilitar a entidades que las utilizan, para recabar con respeto datos de carácter íntimo.

Estos requisitos enmarcados al principio de legalidad serán menos estrictos, en relación a los datos personales que no tengan un carácter sensible, será suficiente

que las cargas informativas impuestas a personas y la utilización que se mantiene de su propia información, tenga amparo deficiente.

La autora Celeste Gay menciona que: "La exigencia del tema y de una reserva formal puede estar preceptuada por consideraciones en el uso adecuado de la información, es evidente asumir la responsabilidad a la estructura en el manejo de los datos, la obtención de información, tratando de sistematizar y regularizar su protección, desde una obtención por suministro, cuando es una norma jurídica la que crea el deber de informar y por aparte, la información por captación, cuando el deber de aportar información surge de la actividad económica."[19]

En relación a lo anterior citado, como formas de proporcionar información por cualquier entidad, gran parte de la doctrina afirma que los deberes de responsabilidad en el trato, tienen naturaleza de deberes públicos de prestación, de carácter personal, así como de la protección constitucional, teniendo como establecimiento y régimen jurídico básico, estar cubierto por la reserva formal de ley.

2.6. Vías de acceso a información privada de tipo personal

Los accesos a la información se han perfeccionado en el transcurso de los años, desde una simple hoja de papel en la cual se consignaban datos más generales,

[19] Gay Fuentes, Celeste. **Intimidad y tratamiento de datos en las administraciones públicas.** Pág. 37.

hasta una alta y más sofisticada tecnología digital y difusión de datos por medios inteligentes y sistematizados, que permiten la utilización, manejo y transporte de información en el menor tiempo.

Por otro lado, existe un mundo tecnificado, desde los satélites que transmiten datos utilizando satélites orbitales que funcionan como estaciones de relevo para transmitir señales de microondas a través de distancias muy grandes; hasta la utilización de teléfonos celulares, que funcionan utilizando ondas de radio para comunicarse con antenas de radio ubicadas dentro de áreas geográficas adyacentes llamadas celulares.

También existen redes inalámbricas diseñadas explícitamente para transmisión de archivos de datos en dos vías llamadas redes móviles de datos que, basadas en radio transmiten datos hacia y desde computadoras portátiles; un tipo de red móvil de datos se basa en una serie de torres de radio construidas específicamente para transmitir texto y datos. Existe a su vez la transmisión de datos a través de medios inalámbricos, que envía señales por medio del aire o el espacio sin necesidad de una línea física, utilizando un espectro electromagnético.

Como lo establece el autor Guido Miranda: "La tecnología misma da las soluciones para promover la protección de los derechos humanos por internet, por medio de sistemas de protección de la intimidad como la criptografía o la estenografía, o bien, por medio de la creación de nuevas vías de acceso a la información, espacio de participación ciudadana, transparencia, creación de comunidades virtuales de

intercambio de bienes, servicios e ideas, y nuevos canales más democráticos de difusión informática y cultural a través de los cuales también se pueden transmitir obras protegidas por los derechos de la persona."[20]

De lo anteriormente citado, se hace alusión a que la tecnificación de la información permite una utilización peligrosa de los datos personales por medios electrónicos o sistemáticos, se manejan muchos aspectos que a su vez no están del todo protegidos; en esa virtud, el manejo de los datos y su fácil acceso por parte de cualquier institución, sin previa autorización de la misma persona, hace vulnerable que se abuse de la misma.

El uso de medios como internet pueden ser objeto de manipuleo por cualquier persona con mala intención que afecte a cualquiera; sea cual fuere el caso, el potencial de invasión de la privacía por este medio es considerable, que es el medio que utilizan las empresas por ejemplo para la transportación de la información; o sea, las personas que pueden emprender tal invasión varían desde *hackers* delincuentes hasta compañías de mercadotecnia, ya que existe información acerca de todos, disponible sin consentimiento o autorización.

Como bien lo mencionan los autores Stair y Reynolds acerca de la personalización y la utilización de los datos de información: "Hoy son cada vez más las compañías que buscan tener una relación más estrecha con sus clientes mediante el uso de internet. Por otra parte, la sensibilidad incrementada a los problemas de protección

[20] Miranda Gutiérrez, Guido. **La seguridad social y el desarrollo en Costa Rica.** Pág. 13.

de la privacía ha hecho que incluso las empresas más ambiciosas procedan con cautela."[21]

Así, las vías de acceso a la información son puertas abiertas por medios electrónicos, que utilizan información de datos personales para el propio fin e interés de quien los manipula.

Se finalizan de esta manera los puntos más importantes del desarrollo de los datos personales, su acceso y quién los utiliza, teniendo por sobre entendido las fuentes de manejo y captación, los controles que a su vez deben tener, así como la exposición más importante de las normas de mayor auge para la protección de los mismos, cómo debe ser manejada su reserva legal, para así tener la mejor base de fundamentación y solución del problema.

[21] Stair, Ralph M. y George W. Reynolds. **Principios de sistemas de información: enfoque administrativo.** Pág. 649.

CAPÍTULO III

3. Conflictos de datos personales en las empresas privadas

Un conflicto es la consecuencia de la diferencia entre dos formas distintas de pensar; dirigido al tema, es un problema de presunción con respecto a la posible mala utilización de información de carácter personal, en que se ven afectados los múltiples ámbitos de la vida de un individuo.

Hay que iniciar con el problema de la utilización de bases de datos por empresas privadas; recordando como bien lo menciona la autora Vicky Elías: "Un sistema de base de datos es básicamente un sistema computarizado para guardar registros, cuya finalidad general es almacenar información y permitir a los usuarios recuperarla y actualizarla con base a peticiones"[22]

De esa cuenta, una base de datos es un conjunto de datos persistentes que es utilizado por los sistemas de aplicación de alguna entidad; en el sector público lo denominan banco de datos. Ahora bien, los conflictos surgen por la mala utilización que les dan las empresas privadas, lo que ocasiona algunas veces litigios.

[22] Elías Pérez, Vicky Aracely. **Violación del principio de inocencia por personas que manejan bases de datos.** Pág. 79.

3.1. La afectación en los ámbitos económicos y sociales

En la mayoría de casos, las entidades cualquiera que sea su actividad económica o social tienen un fin, el trato y vinculación con personas, estas entidades elaboran reportes de personas que contienen información general, comportamiento de pago, referencias comerciales, datos legales, historial laboral; creando así, un tipo de perfil que les proporcione una idea de la persona.

Tomando un ejemplo de la realidad, la empresa Transunión Guatemala, es una entidad que recopila toda clase de información y proporciona el servicio de consulta por medios electrónicos o vía internet; dentro de su accionar como negocio se pueden encontrar reportes diarios de procesos anotados en los tribunales, registros de marcas y patentes, números de identificación tributaria, avisos inmediatos, etc.

Otra entidad dedicada a la actividad de la difusión de datos o bases de información personal es Infornet, que brinda información como antecedentes penales, historial crediticio; además, decide los requerimientos de otras personas; por ejemplo, da la pauta para que se autorice o no un crédito o un préstamo bancario, afectando así a una gran cantidad de personas, que en su mayoría no tienen ni idea de la existencia de tal información.

Por ese motivo es que todo el manejo de la información crea problemas para algunas personas, pues no se brinda seguridad de la información que se tenga y

en muchos casos ésta no está actualizada, creando así desconfianza hacia las personas tanto en su actividad personal como en la comercial o laboral; además, esto ocasiona también la reducción de oportunidades determinantes, como la adquisición de un empleo; por ejemplo, o bien el logro de un crédito o préstamos de dinero.

Por eso es que hay que tomar en cuenta un aspecto muy importante para no afectar y crear motivos de discusión ni violación a la intimidad en la utilización de datos personales, y debe ser la responsabilidad del encargado de la protección de los mismos; tomando en cuenta primero las disposiciones de ley sobre protección de datos así como las normas administrativas de la empresa que hacen uso y distribución de los datos; quienes en el ejercicio de la función deben tener un control respecto de la protección de éstos, de preferencia que el encargado de los datos sea independiente a la empresa, con gran sentido de ética, sobre el tipo de datos y en la medida en la cual realizará la labor en el manipuleo de los mismos.

Esta independencia mencionada, se puede establecer como de interés público y personal; por otra parte, deben tener control de los centros procesadores de datos, estando obligados a asistir al encargado de la protección de datos y sus colaboradores en el cumplimiento de su cometido; deben a su vez, proporcionar información, respondiendo a preguntas, permitir el examen de documentos y datos almacenados, y acceso a todas las oficinas.

Asimismo, el encargado deberá elaborar un informe escrito sobre los resultados de su control, tomando en cuenta que las personas deben tener conocimiento de las bases jurídicas de la recolección de datos; también en la transferencia de datos a otros interesados, deben indagar si éstas se han realizado dentro del marco de las disposiciones legales, o si se contaba con el consentimiento válido de los afectados.

Tomando de ejemplo, que contrario al tema de la seguridad de los datos, fuese su destrucción, si una desmaterialización de documentos se realiza en forma adecuada, o si la seguridad está suficientemente garantizada en un programa de procesamiento de datos y en redes informáticas, como para impedir que personas no autorizadas accedan a datos personales o evitar pérdida de datos, crearía menos conflicto que su misma utilización.

Debe tenerse en cuenta que, cuando los controles detectan violaciones de las normas de la protección de datos u otros defectos en el procesamiento, el encargado de la protección de ellos puede dejar constancia de sus observaciones ante el centro que procesa los datos, y exigir que los defectos sean subsanados dentro de un plazo adecuado; en este sentido, los defectos son informados a los supervisores del centro controlado.

La afectación en los ámbitos económicos y sociales para tomar una decisión de escogencia en relación a áreas de oportunidad para personas individuales por el manejo de su información íntima, debe ir ligada a todo este tipo de tareas y al

derecho de protección de datos, que está sujeto a grandes desafíos como la eficiencia, economía y particularmente la rapidez con que se manejan, evitando una tergiversación en la información y la oportunidad de un individuo.

3.2. Creación de bancos de datos sin autorización para su publicación

Actualmente la tecnología moderna está al alcance de la mayoría de personas; por ejemplo, una cámara de video, un teléfono celular, internet, correo electrónico, tarjetas de crédito, etc., de esa cuenta la tecnología enlazada puede constituir un peligro por su poca seguridad y bienestar en su momento, utilizada para violar la intimidad de las personas.

Como bien lo menciona el sociólogo David Lyon: "Existen dos factores que amenazan la intimidad desde hace un par de décadas. Primero, que el almacenamiento y la difusión a gran escala de datos personales es cada vez más fácil. El segundo, que algunas informaciones que antes se consideraban triviales, como por ejemplo, los gustos, tallas, número de hijos, entre otros, ahora tienen un valor en el mercado y son buscadas con avidez por quienes desean obtener ventajas comerciales de ellas."[23]

De lo anteriormente citado, se puede deducir que todo este tipo de información es utilizada o puede ser usada por cualquier persona y por cualquier medio, así por ejemplo las empresas, la utilizan para obtener cierto tipo de ventaja para la

[23] Lyon, David. **El ojo electrónico: el auge de la sociedad de la vigilancia.** Pág. 299.

elección de determinado interés, información que sin autorización y en varias ocasiones sin consentimiento se administra. A continuación se expondrán los perfiles que manejan determinadas empresas.

3.2.1. Perfiles de bases de datos utilizados por empresas

Los perfiles de las personas que contienen las bases de datos son diferentes de acuerdo a la empresa o entidad que los utilice, pero generalmente son los siguientes:

Empresas que utilizan información de bases de datos de forma internacional:

a. Nombre de la persona
b. Número de cédula de vecindad
c. Lugar de nacimiento
d. Fecha de nacimiento
e. Número de identificación tributaria
f. Ocupación
g. Direcciones
h. Teléfonos
i. Nombre de sus padres
j. Empresas que posee
k. Representación que ejerce de alguna entidad
l. Bienes que posee
m. Juicios, en cualquier estado del proceso en que se encuentre

n. Nombre de los bancos a que éste se encuentre afiliado
o. Vehículos que posee
p. Antecedentes penales

Como se puede ver, es información personalísima, utilizada para clasificar de algún modo el estatus de la persona individual que goza de derechos y obligaciones, y a toda esta información se puede tener acceso por medio de faxes o internet a nivel mundial.

3.3. Información y documentos con datos personales que requiere una empresa privada

Se inicia este punto, tomando como ejemplo alguna entidad reconocida internacionalmente dedicada a la creación de bases de datos, que cuando una persona social como ente empleador requiere sus servicios, consulta su base de datos pero la persona a contratar no se encuentra en la misma, entonces solicita a la entidad dedicada a ese fin que investigue, quienes inician en tribunales bajo el argumento que todos los juicios son públicos, averiguan si la persona a contratar tiene alguna situación jurídica que solventar; en otros casos, los bancos del sistema faltan a la reserva de la confidencialidad con sus clientes, al proporcionar informaciones incompletas de sus usuarios.

Aumenta más el abuso de la información personal, cuando se hacen clasificaciones, como por ejemplo si la persona a contratar es de algún tipo de

religión, raza, o nacionalidad, y por lo mismo no es tomada en cuenta, siendo probablemente la más idónea para el cargo u obligación a desempeñar, y si existe ausencia de información, las personas se ven obligadas a administrar únicamente la poca información que se tiene, por lo que se ajustan y buscan crear una efectiva base de datos que responda a las necesidades y objetivos buscados; asimismo, se busca enlazar información de otras fuentes creadas que permitan complementar los datos que se necesitan. Si existe total ausencia de información se deben buscar los mecanismos legales para la obtención y creación de la nueva base de datos.

Como ordinariamente son entidades públicas las que requieren información para controlar a su personal, las empresas privadas necesitan para su funcionamiento y para el ejercicio de sus actividades, el acopio de grandes cantidades de información relativa a personas; por lo tanto, tal como lo menciona Alva Garriga: "Se ha convertido en una activo más de las empresas, en algunas, en el más valioso."[24]

En algunos casos también, se trata de empresas que almacenan datos personales en virtud de la existencia de una relación contractual o laboral con el titular y; en otros, las empresas a su vez recogen datos de carácter personal para otras empresas; entonces, la finalidad de la empresa no es proporcionar una relación sino únicamente información para otras empresas.

[24] Garriga Domínguez, Ana. **Tratamiento de datos personales y derechos fundamentales.** Pág. 158.

3.4. Comisión de delitos por el mal manejo de procedimientos y manipulación de información

Como se ha mencionado en el desarrollo de la presente investigación, las leyes de protección de datos deben amparar sobre todo la intimidad. Por lo tanto, tomando en cuenta las ideas hasta ahora expuestas, se debe recordar el uso de los principios que orientan una legislación de este tipo; así siguiendo los lineamientos del autor Renato Jijena: "Se hace necesario regular la recolección de datos nominativos, determinándose cuáles tienen el carácter público con el resto y que afecten a una persona."[25] Es decir, deben estar dirigidos también a datos de carácter personalísimo y que involucren el interés de ambas partes, estableciendo que el procedimiento de registro de datos debe estar previamente garantizado.

En la comisión de un hecho en el cual se deba determinar el abuso sobre la información, es difícil establecer el momento; o sea, el preciso instante en que se está manejando errónea e intencionalmente la información, en forma general se podrían denominar atentados contra la privacidad e intimidad que realizan empresas privadas; en tal caso, de estar ese momento tipificado como tal, produce una consecuencia, una sanción; a su vez, no debe ser difícil constatar que aquéllos son cuantitativamente cada vez más numerosos y cualitativamente más diversos.

---

[25] Jijena Leiva, Renato Javier. **Chile, protección penal de la intimidad y el delito informático.** Pág. 51.

En el ámbito del derecho penal reviste mayor importancia la construcción de una teoría jurídica de la intimidad, ya que el concepto material de todo bien jurídico tutelado desempeña el papel de límite del ius puniendi, esa facultad del Estado para definir cuáles conductas merecen ser amparadas y; en consecuencia, establece las que atentan contra el patrimonio privado e íntimo de una persona, que se ve afectada en la toma de decisiones en una posible relación laboral por ejemplo. Por lo tanto, la comisión de un delito conlleva la utilización de medios informáticos cualquiera que sea su tipo, haciendo énfasis especial que en materia de protección a la intimidad debe ser sancionada su abuso.

3.5. La falta de intervención del Estado en las políticas, manejo y controles de la información de datos personales

Son muchas las causas que originan la irresponsabilidad del manejo de datos personales; siendo responsabilidad y obligación del Estado, velar por la seguridad jurídica del uso de la información de carácter personal, así como las medidas a adoptar para prevenir su mal uso o abuso.

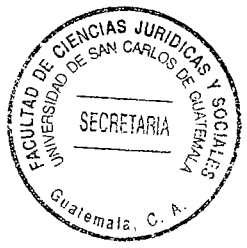
Si bien es cierto, un punto importante es que la seguridad no debe ser vulnerada por ningún precepto, los malos manejos o abuso de la información personal, traen como consecuencia la obligación de reparar el daño, por quien lo ocasione dolosa o culpablemente, tomando en cuenta cualquier tipo de perturbación, mal trato, abuso de la intimidad de las personas, que se cause por indiscreción, impertinencia, codicia o insensatez, así como por la falta de compromiso en el

manejo de la utilización de bases de datos, que afecten personalmente todos los aspectos inherentes al individuo.

Para que el Estado se vea involucrado en el resarcimiento del abuso en el manejo de datos por empresas privadas, se hace necesario que tales acciones sean también consideradas como delitos o al menos cuasidelitos, ya que como menciona el autor Jijena: "La configuración del delito informático como una figura punible distinta, es la única solución que permitirá resolver el problema desde el punto de vista del hecho ilícito."[26]

Es así, que la falta de intervención y control del Estado sobre las empresas privadas que manejan datos de los individuos, es la falta de medios de defensa de los mismos; y como se ha mencionado en el transcurso de la presente investigación, la utilización del derecho al *habeas data* o a la llamada autodeterminación informativa, debe adquirir presencia fundamental y significativa tanto en el texto constitucional como en la ley ordinaria, ya que como se ha preceptuado es el mecanismo de defensa ideal por el cual se le dará acción al Estado mediante el organismo correspondiente, permitiendo a las personas contar con un mayor escrutinio sobre sí mismas y ejercer un mayor control sobre la actividad de las autoridades públicas y de las empresas privadas en el manejo de datos.

[26] Jijena. **Ob. Cit.** Pág. 52.


FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Guatemala, C. A.

CAPÍTULO IV

4. Soluciones al acceso de datos personales

En virtud del análisis jurídico expuesto se proponen algunas soluciones, que traten principalmente de coordinar y mantener una autorregulación y que se especialicen en el manejo y creación de bases de datos que son de uso diario de empresas privadas y que afectan a las personas en todo aspecto de su vida, tomando en cuenta que existen espacios sociales también involucrados, donde concurre descontrol y manejo indiscriminado de los datos personales.

4.1. Bancos de datos en donde se califique y clasifique la información

Dentro de la diversidad de la información manejada en bases electrónicas de almacenamiento, existe la presunción de legalidad de su existencia, al mismo tiempo de la confiabilidad de la misma, en cuestiones de interés para los particulares.

La calificación y clasificación debe hacerse con apego al derecho, pero al derecho individual de protección a la intimidad de los individuos como una garantía especializada, o sea de carácter especial, dentro de la cual el mismo Estado está en la facultad y obligación de prever la mala utilización y tergiversación de la información que pueda perjudicar al individuo.

Así pues, en la utilización y calificación para la clasificación, debe otorgarse a los datos cierto grado de seguridad, en la cual exista el mejor y eficaz control de la información dentro de la base de datos. Este grado de seguridad deberá enmarcar aspectos como la creación de un marco legal consistente y general, para facilitar la elaboración y adopción de medidas técnicas y organizativas que refuercen las garantías en el tratamiento de los datos personales.

Dentro del marco legal se debe regular que la clasificación de datos personales propiamente debe estar protegida, y acotar los diversos extremos de aplicación de la normativa en la materia, para establecer aquellos datos que serán ofrecidos a conocimiento de las empresas o del público en general.

La regulación nacional y la internacional deben ser congruentes recíprocamente, ya que la aplicación a todos aquellos datos que sean considerados personales, y mediante los cuales se obtenga información de alguna persona para cualquier fin, debe proteger la misma posibilidad de identificarla y verificar la confiabilidad de los datos; en tanto que la normativa debe regular y proteger los datos personales, ya que tal aplicación se presenta en sectores privados y públicos.

En la actualidad todo el manejo y uso de datos a través de soporte técnico y sistemático, de programas corporativos, programas de correo electrónico, etcétera, deben ser también protegidos según el uso e interés de entidades públicas o privadas.

Así también, se debe crear una norma específica que regule todos los tipos de ficheros, por ejemplo: los del régimen electoral, los ficheros de videocámaras de seguridad, los derivados del registro civil de personas; es decir, debe regularse una norma especial de control, dependiendo el tipo de fichero.

4.2. Legalidad del manejo de datos personales por empresas privadas

Ya quedó claro que actualmente el manejo de datos permanentes por parte de empresas privadas ha generado todo tipo de intromisiones en la vida personal de cualquier individuo, no respetando el honor, la intimidad y la propia imagen de las personas, considerándose estas intromisiones ilegítimas, a pesar de que se encuentran autorizadas presuntamente por la autoridad competente y por autoridad administrativa de una empresa.

El principio de reserva legal en materia de límites a libertades públicas en la utilización de los datos para iniciar una relación laboral, es abusada en su utilización. Por eso es necesaria la creación de una norma de tipo especial que permita a la administración pública controlar los datos de carácter íntimo, y su utilización en ámbitos de aplicación de trabajo que afecten el interés de quienes aspiran al mismo.

Además, se debe regular el uso de una reserva de tipo legal y formal, que administre la obtención de información, sistematizando la regulación de las mismas potestades de obtención de información que son encomendadas a

instituciones que abusan en la utilización de ésta. Los controles legales que se establecen son importantes para la seguridad jurídica de las personas en relación a la información personal que es necesaria para la realización de negociaciones o como parte de los requisitos esenciales que requieren la empresas privadas, comprometiéndose así las instituciones contraloras de los datos a su buen uso y manejo, evitando la corrupción o filtración de la información almacenada.

En la recopilación de los datos y la legalidad de su manejo es imperativa la utilización de una ley o leyes con carácter de obligatorias, imponiendo la obligación de lealtad al responsable de la creación de una base de datos personales, prohibiendo a su vez la creación de éstos fuera del marco legal.

Los requisitos de las bases de datos utilizados para crear una relación laboral, deben ser establecidos bajo el principio de legalidad; en el cual, como ya se mencionó en apartado anterior, se encuentra uno de los pilares más importantes de la normativa en materia de protección de datos de carácter personal, dirigidos a crear una relación de trabajo; tal información, debe ser para el empleador, no sólo un deber sino que debe ser configurado como un derecho inherente al contratado, así como el deber de poner en conocimiento de este último el proceso de recolección.

4.3. Importancia de la creación de una normativa que regule la calificación y clasificación de datos personales

Dentro de las gestiones de tipo administrativo que utilizan las empresas para cumplir con el conjunto de obligaciones respecto a los empleados, está la de recabar y almacenar una gran cantidad de datos personales, los cuales introducen en programas específicos que facilitan su depuración y selección, que en el presente caso utilizan para seleccionar o elegir a las personas idóneas para determinados trabajos, lo cual es ilegal pues seleccionan a las personas por su religión, sexo, edad, experiencia, etc.

Consecuentemente, no existe respeto en la utilización de la información personal, no sólo porque a veces es incorrecta o desactualizada sino que la puede obtener cualquier persona o empresa para contratar a sus trabajadores. Por eso es importante la creación de una ley que regule el uso y clasificación de datos personales, ya que en realidad no existe control sobre las empresas que manejan estas bases, quienes abusando de la información que poseen no han respetado el derecho a la intimidad de las personas..

Además, las empresas privadas que se dedican a esta tarea deben ser obligadas por ley a respetar los principios de información y consentimiento, que es el permiso o autorización que una persona otorga para que las empresas proporcionen sus datos personales a otras empresas que así lo requieran por cuestiones de trabajo, personales o económicos.

4.4. Creación de una institución gubernamental para la protección de datos personales

Ahora bien, de nada sirve la creación de una normativa que controle el uso de las bases de datos si no existe una institución que se encargue de hacer respetar dicha normativa.

La Constitución Política de la República de Guatemala, regula que deben existir organizaciones dedicadas a la defensa de los derechos inherentes a las personas, pero éstas no han sido capaces de resguardar la utilización de ficheros integrados por una base de datos de carácter personal.

Por lo tanto, resulta necesaria la creación de un acuerdo de protección de información personal, y de una entidad pública o gubernamental, que vele por la creación y manejo de las bases de datos de toda índole, en especial los utilizados por empresas privadas, que muchas veces desvirtúan el proceso de selección, convirtiéndolo en discriminatorio y abusivo.

También, debe conformarse un registro que resguarde la integridad de la información de las personas individuales, que sea de carácter general y público, donde se inscriban las bases de datos creadas por instituciones privadas, o por las mismas empresas contratantes, donde exista un departamento de inspección de empresas que utilicen bases de datos que fiscalicen la utilización de las mismas así como el proceso de selección.

Este registro de bases de datos, debe tener claro el concepto del derecho a consultas de datos de carácter personal, sus finalidades y la identidad del responsable de la creación de las bases de datos, respetando el derecho de acceso a la información personal, que actualmente ha sido desvirtuado por las empresas privadas que se dedican a este negocio.

El registro público, inscribiría los mecanismos efectuados en la creación de bases de datos, con indicación de sus características y marco legal, incorporando todos y cada uno de los datos sometidos, es así que el creador de las bases de datos está obligado a notificar para la inscripción la información referida a la existencia de un fichero contenido de datos personales; teniendo la persona como consultante el derecho a conocer los datos contenidos en el fichero, utilizados para la obtención de cualquier tipo de empleo.

La legislación que se propone encomendar al Estado en materia de protección de datos personales, debe exigir la tenencia de un registro de accesos a los datos contenidos en un fichero, fiscalizados por un registro general de protección de datos personales; en el cual, como se mencionó antes, se inscribirían las bases de datos creadas; y una agencia de fiscalización o control, que esté encargada de la fiscalización física en la utilización del proceso de selección de personas en empresas privadas.

4.5. Análisis en el manejo de datos personales en los ámbitos económicos y sociales para la solución de conflictos

Como se analizó en el transcurso de la presente investigación, la importancia del manejo de bases de datos integrados por información de carácter personal es de impacto social, y el marco jurídico debe orientar su protección sobre fundamentos previamente establecidos y concretos, en los cuales se verifique el respeto y la integridad de las personas afectadas por el manejo de tal información, que repercute en todos los aspectos de la vida.

La normativa debe ir encaminada a que, la protección de los datos constituye un elemento importante para la implementación de la misma democracia; dentro de la fundamentación mencionada, se debe exponer que quienes no pueden saber con suficiente certeza, cual es la información acerca de su persona y su entorno social; quienes no están en condiciones de estimar el conocimiento de sus potenciales exponentes, quienes pueden experimentar serios impedimentos en su libertad de concebir decisiones basadas en ficheros de información personal, serán afectados por la mala utilización, siendo discriminatorio tal proceso, aunado al abuso al derecho de intimidad de la persona.

El mismo derecho de autodeterminación informativa y el espíritu de la norma jurídica a crear, es irreconciliable con un orden social en el cual la persona individual afectada no puede estar informado sobre quién sabe qué cosa y en qué ocasión, acerca de él o ella misma; esto enmarca un problema en los aspectos

sociales de los individuos, quienes viven con la duda de saber si sus propias conductas típicas o atípicas se registran en todo momento, o si están siendo de cierta forma fiscalizados por lo que puedan o no tener, qué les gusta, qué religión practica o hasta su propia orientación sexual, por ejemplo.

Por otro lado, el II Encuentro Iberoamericano de Protección de Datos, celebrado del 2 al 6 de junio de 2004 en La Antigua, Guatemala se enmarcó dentro de ese objetivo prioritario. Reunió en esta ciudad a representantes de Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, España, Guatemala, México, Nicaragua, Paraguay, Perú, Portugal, Uruguay y de la Conferencia Iberoamericana, para poner en común los conocimientos y experiencias planteados en relación al proceso de implementación de la normativa de protección de datos personales. Dentro de las jornadas se tuvo la oportunidad, por ejemplo, de escuchar de primera mano cuáles eran los entronques de este derecho en la legislación constitucional de cada Estado y qué soluciones se habían instrumentado desde la jurisdicción para proteger los derechos de los ciudadanos frente al uso abusivo de sus datos personales.

Este Encuentro fue organizado por la Agencia Española de Protección de Datos. Sin embargo, hay que resaltar el enorme apoyo prestado por la Agencia Española de Cooperación Internacional y por la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas, sin cuya colaboración seguramente no hubiera sido posible su celebración.

Se cree que este Encuentro ha marcado un punto de inflexión en las relaciones iberoamericanas en materia de protección de datos, ya que a partir de la Declaración de La Antigua, se constituyó la Red Iberoamericana de Protección de Datos, abierta a la incorporación de representantes de todos los países iberoamericanos, punto de encuentro y canal permanente de diálogo y colaboración entre sus miembros. Además, la citada Declaración sirvió para que los Jefes de Estado y de Gobierno reunidos en Santa Cruz de la Sierra, incluyeran en su Declaración Final un apartado, el 45, por el que reconocieron el derecho fundamental a la protección de datos de carácter personal.

Destacan como objetivos de la Red, promover la cooperación interinstitucional y el diálogo entre actores claves para el desarrollo de iniciativas y políticas de protección de datos, así como promover políticas, tecnologías y metodologías que permitan garantizar el derecho fundamental a la protección de datos personales.

A partir de ese momento, la Red se convirtió en un foro de promoción del derecho fundamental a la protección de datos en esta comunidad, cuyo impulso y responsabilidad asumieron también los responsables políticos de los respectivos Estados signatarios de la Declaración de Santa Cruz de la Sierra.

La consolidación definitiva de este foro como cauce idóneo para la toma de sus decisiones, adopción de documentos y fijación de sus estrategias futuras se

convierte en uno de los objetivos estratégicos de la Red. De tal forma que, es interés primordial de las instituciones que en la actualidad la constituyen, el impulso e implantación del derecho fundamental a la protección de datos de carácter personal a través de las entidades con capacidad y competencias para instar a los gobiernos nacionales a que elaboren una regulación normativa en esta materia a efectos de lograr la obtención de la Declaración de Adecuación por parte de la Comisión Europea.

Los objetivos y la organización de la Red quedan recogidos en el Reglamento aprobado con motivo del VI Encuentro Iberoamericano de Protección de Datos celebrado en Cartagena de Indias, Colombia, del 27 al 30 de mayo de 2008.

En consecuencia y a fin de cumplir con su cometido, desde su creación la Red ha celebrado anualmente siete Encuentros Iberoamericanos. Estos Encuentros se constituyen como foros de discusión directa y adopción de acuerdos y decisiones de la Asamblea General conformada por los países miembros. Desde sus inicios, estos foros han permitido apreciar el creciente interés, preocupación y compromiso en materia de protección de datos en los países iberoamericanos en un asunto tan sensible para los ciudadanos.

El hombre como titular de derechos debe defenderse de las injerencias indebidas de los poderes públicos, sus órganos, sus agentes y de los ataques a la intimidad causados por otros individuos.

Tan relevante es la preservación de este derecho que ha sido consignado en el Artículo 12 de la Declaración Universal de los Derechos Humanos del 10 de diciembre de 1948, que establece: "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". De la misma manera se le menciona en el Artículo 11 del Pacto de San José de Costa Rica, que establece: "Protección de la Honra y de la Dignidad Inciso 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación".

Este derecho, se encuentra consagrado en diversas constituciones como en la Constitución de la República de Paraguay en el Artículo 33, que indica: "La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas".

En la Constitución de la República de Honduras en el Artículo 76, que establece: "Se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen"; y también en la Constitución Política del Ecuador en el Artículo 23 inciso 8 que establece: "El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona".

En este Artículo se puede apreciar que es deber del Estado resguardar un ambiente propicio para el desarrollo personal y garantizar el desenvolvimiento familiar. La legislación ecuatoriana protege el nombre de la persona, evitando así el uso indebido del mismo, porque éste ayuda a la fácil individualización de la persona. El titular del nombre puede cambiarlo si tiene un homónimo que tenga una fama que produzca malestar en la sociedad. Nadie puede utilizar el nombre propio para fines comerciales, artísticos, delincuenciales, etc.

Así también, existen mecanismos que protegen la información directamente vinculada con cuestiones privadas, relativas a la intimidad de la persona que no pueden estar a disposición del público. Estos se orientan a preservar y resguardar aquella información con el principal objetivo de que los datos no se almacenen, ya que esta información pertenece sólo a la propia persona.

El uso de la información almacenada, procesada o distribuida a través de cualquier medio físico debe respetar el honor, la privacidad, y el goce completo de

los derechos. Así, deben impedirse las intromisiones perturbadoras y la inadecuada difusión de datos cuando se afecta la esfera íntima, tanto familiar como personal. Por esto se han creado recursos especiales para proteger los datos que afecten a la honra o a la intimidad como el "habeas data".

Por ejemplo, el habeas data está regulado en el Artículo 94 de la Constitución Política del Ecuador, que dispone que: "Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar al funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización..."

El hábeas data permite a toda persona acceder a registros públicos o privados, en los cuales están incluidos sus datos personales o de su familia, para requerir su rectificación o la supresión de aquellos datos inexactos que de algún modo le pudiesen perjudicar en su honra, buena reputación e intimidad.

El derecho a la protección de datos implica, a su vez, el derecho a conocer la existencia de ficheros o de información almacenada y el propósito o la finalidad que se persigue con ellos; el derecho a acceder, que permite a los afectados

averiguar el contenido de la información registrada, o participar de la información que sobre la imagen o concepto de ellos se tenga; y el derecho a rectificar, que es la posibilidad del titular afectado de que los datos sobre su persona al ser incorrectos, inexactos u obsoletos sean rectificados en la medida en que, al ser ajenos a la realidad, le pueden causar perjuicio".

Por último cabe resaltar que el Estado es el obligado a proteger el accionar de empresas privadas, en la creación y uso de información que contenga datos personales, ya que está desprotegida por un orden fiscalizador y público, que mantenga el control no sólo de las empresas sino de la información que utilizan, para que se respete así el derecho de la intimidad de toda persona, que protege la Constitución Política de la República de Guatemala.


FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Gualemala, C. A.

CONCLUSIONES

1. No existe una ley específica que proteja la creación de bases de datos de información personal, utilizados por empresas privadas que violan así el derecho a la intimidad de las personas.

2. Existe simulación en procesos y mecanismos no regulados que permiten obtener información de bancos de datos personales, los cuales son utilizados por quienes los crean o las empresas privadas para clasificar indiscriminadamente a las personas.

3. Las empresas que usan los datos personales se han hecho millonarias, pues cada consulta a su base de datos tiene un costo, aunque la información sea ajena a ellos.

4. No existe un control formal sobre las empresas que manejan bases de datos en relación a la información que almacenan y su veracidad, así como la actualización de las mismas, estableciendo así datos que son manipulables y nada fidedignos que al ser consultados sólo vulneran los derechos de las personas.


FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Guatemala, C. A.

RECOMENDACIONES

1. Instituir por parte del organismo legislativo, una ley de carácter específico que proteja la creación, recopilación y utilización de bases de datos de carácter personal, utilizadas por empresas privadas que tienen acceso a la intimidad de las personas.

2. El Estado debe crear un registro público obligatorio, una procuraduría o una dirección de asistencia y protección a los datos personales, que se encargue y regule los procesos y mecanismos de obtención de la información de carácter personal utilizado por empresas privadas, para evitar la discriminación de toda índole hacia las personas.

3. Las empresas privadas que manejan datos personales obligatoriamente deben rendir cuentas e informes a la Superintendencia de Administración Tributaria y la Contraloría General de Cuentas, pues por cada información que proporcionan cobran un precio sin extender factura o comprobante de pago.

4. Que las empresas privadas que creen o utilicen bases de datos personales, también sean reguladas por la Ley de Acceso Público a la Información, de modo que cualquier persona tenga acceso a dicha información no sólo para actualizar sus datos sino para evitar la mala utilización de los mismos.


FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
Guatemala, C. A.

BIBLIOGRAFÍA

ALMUZARA ALMAIDA, Cristina. **Estudio práctico sobre la protección de datos de carácter personal.** España: Ed. Lexnova, 2007.

AZOFEIFA DELGADO, Hernán Esteban. **Los sistemas de información electrónicos, el derecho a la intimidad y el derecho penal.** Costa Rica: Ed. Universitaria, 1993.

CANO MORALES, Rodrigo. **Acción de habeas data como mecanismo de protección jurídica de los datos personales.** Guatemala: Ed. Mayte, 2004.

DALLA VÍA, Alberto Ricardo. **La conciencia y el derecho.** Argentina: Ed. Fundación Editorial de Belgrano, (s.f.).

DEL PESO NAVARRO, Emilio. **Ley de Protección de Datos: la nueva LORTAD.** España: Ed. Díaz de Santos, 2000.

ELÍAS PÉREZ, Vicky Aracely. **Violación del principio de inocencia por las empresas que manejan bases de datos personales.** Guatemala: Ed. Mayte, 2007.

GARRIGA DOMÍNGUEZ, Ana. **Tratamiento de datos y derechos fundamentales.** España: Ed. Dyckinson, (s.f.).

GOZAÍNI, Osvaldo Alfredo. **Habeas data, protección de datos personales, doctrina y jurisprudencia.** Guatemala: Ed. Mayte, 2004.

GAY FUENTES, Celeste. **Intimidad y tratamiento de datos en las administraciones públicas.** España: Ed. Complutense, 1995.

HERNÁN ORTIZ, Ana Isabel. **El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales.** España: Ed. Dykinson, 2002.

JIJENA LEIVA, Renato Javier. **Chile, protección penal de la intimidad y el delito informático.** Chile: Ed. Universitaria, 2000.

LYON, David. **El ojo electrónico: el auge de la sociedad de vigilancia.** España: Ed. Dykinson, (s.f.).

MADEC, Antonio. **El mercado internacional de la información, los flujos transfronteras de información y datos.** España: Ed. Fundesco, 1984.

MARTÍNEZ Y MARTÍNEZ, Ricardo. **La memoria contra el olvido.** España: Ed. Plaza y Valdez, 2005.

MIRANDA GUTIÉRREZ, Guido. **La seguridad social y el desarrollo en Costa Rica.** Costa Rica: Ed. Universitaria, 2006.

PIÑOL RULL, Osman y Oscar Estadella Yuste. **La regulación de la transmisión internacional de datos.** España: Ed. Dykinson, 2001.

PUCCINELLI, Raúl. **El habeas data en el constitucionalismo indo iberoamericano finisecular, en el amparo constitucional.** España: Ed. Dykinson, 2002.

SÁNCHEZ BRAVO, Álvaro A. **La protección del derecho a la libertad informática en la Unión Europea.** España: Ed. Europa, Artes Gráficas, 1998.

STAIR, Ralph M. y George W. Reynolds. **Principios de sistemas de información: enfoque administrativo.** Estados Unidos: Ed. Thompson, 1999.

TÉLLEZ AGUILERA, Abel. **Criminología.** España: Ed. Edisofer, 2006.

UNCTAD, Secretaría de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. **Informe sobre comercio electrónico y desarrollo.** Suiza, Ginebra: Publicación de las Naciones Unidas, 2003.

Legislación:

Constitución Política de la República de Guatemala, Asamblea Nacional Constituyente, 1986.

Declaración Universal de los Derechos Humanos, Organización de las Naciones Unidas. Asamblea General de las Naciones Unidas, 1948.

Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, Convención Europea de los Derechos Humanos, 1953.

Convención Americana sobre Derechos Humanos. Pacto de San José de Costa Rica. Congreso de la República de Guatemala, Decreto número 6-78, 1978.

Declaración Americana de los Derechos y Deberes del Hombre. Conferencia Internacional Americana, Bogotá, Colombia, 1948.

Pacto Internacional de Derechos Civiles y Políticos. Asamblea General de las Naciones Unidas, Resolución 2200ª, 1976.

Ley del Organismo Judicial. Congreso de la República de Guatemala, Decreto número 2-89, 1989.

Código Civil. Enrique Peralta Azurdia, Jefe de Gobierno de la República de Guatemala, Decreto Ley número 106, 1964.

Código Procesal Civil y Mercantil. Enrique Peralta Azurdia, Jefe de Gobierno de la República de Guatemala, Decreto Ley número 107, 1964.

Código de Comercio. Congreso de la República de Guatemala, Decreto número 2-70, 1970.

Código de Trabajo. Congreso de la República de Guatemala, Decreto número 1441, 1971

Código Procesal Penal. Congreso de la República de Guatemala, Decreto número 51-92, 1992.

Código Penal. Congreso de la República de Guatemala, Decreto número 17-73, 1973.