

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

**ANÁLISIS JURÍDICO SOBRE LA NECESIDAD DE REGULAR LA PROTECCIÓN DE
DATOS PERSONALES EN EL COMERCIO ELECTRÓNICO**

JENNIFFER QUETZALI JUÁREZ VALENZUELA

GUATEMALA, SEPTIEMBRE DE 2014

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

**ANÁLISIS JURÍDICO SOBRE LA NECESIDAD DE REGULAR LA PROTECCIÓN DE
DATOS PERSONALES EN EL COMERCIO ELECTRÓNICO**

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

por

JENNIFFER QUETZALI JUÁREZ VALENZUELA

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADA Y NOTARIA

Guatemala, septiembre de 2014

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

DECANO:	MSc.	Avidán Ortiz Orellana
VOCAL I:	Lic.	Luis Rodolfo Polanco Gil
VOCAL II:	Licda.	Rosario Gil Pérez
VOCAL III:	Lic.	Juan José Bolaños Mejía
VOCAL IV:	Br.	Mario Roberto Méndez Alvarez
VOCAL V:	Br.	Luis Rodolfo Aceituno Macario
SECRETARIO:	Lic.	Luis Fernando López Díaz

**TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL**

Primera Fase:

Presidente:	Lic.	René Siboney Polillo Cornejo
Vocal:	Lic.	Edwin Elías Marroquín Azurdía
Secretario:	Lic.	Marvin Vinicio Hernández Hernández

Segunda Fase:

Presidente:	Lic.	Ernesto Rolando Corzantez Cruz
Vocal:	Licda.	Dora Renee Cruz Navas
Secretario:	Licda.	Eloisa Mazariegos Herrera

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 y del Examen General Público).



Guatemala, 26 de mayo del 2014.

Doctor
Bonerge Amilcar Mejía Orellana
Jefe de la Unidad de Asesoría de Tesis,
Facultad de Ciencias Jurídicas y Sociales,
Universidad de San Carlos de Guatemala.
Su Despacho.



Doctor Mejía Orellana:

En cumplimiento de la resolución emanada de la Unidad de Tesis con fecha 6 de junio de 2013 se me designó como asesor del trabajo de tesis de la estudiante **JENNIFFER QUETZALI JUÁREZ VALENZUELA** titulado **ANÁLISIS JURÍDICO SOBRE LA NECESIDAD DE REGULAR LA PROTECCIÓN DE DATOS PERSONALES EN EL COMERCIO ELECTRÓNICO**, por lo que por este medio hago constar que se efectuaron las sesiones de trabajo periódicamente, haciendo las sugerencias que demanda el asesoramiento correspondiente.

El contenido de la tesis en general es eminentemente científico, en virtud que el trabajo realizado deviene de explorar el ámbito de la ciencia y tecnología actual, por ser un tema que ha surgido debido a la modernización de la tecnología y comprende consideraciones sobre la alerta de la defensa del comercio electrónico; ya que el mismo ha avanzado a pasos agigantados, siendo ésta una de las causas que obligan a los países a buscar protección legal para el usuario.

Con relación a la metodología y técnicas de investigación utilizadas; es evidente que se utilizó el método inductivo, porque dicho método lleva al lector a un fin determinado para entender la problemática, situación que se comprueba en el trabajo; también se utilizó el deductivo ya que el trabajo de tesis, tiene los elementos necesarios para deducir los resultados que se sugieren para arribar a las conclusiones señaladas en el mismo; se hace notorio que, la estudiante Jenniffer Quetzali Juárez Valenzuela, hizo uso del método analítico jurídico pues refleja en el análisis que hizo los problemas suscitados en el comercio electrónico.

Licenciado **JUAN ANTONIO MARTÍNEZ RODRÍGUEZ**
ABOGADO Y NOTARIO, Colegiado No. 4803
Avenida Reforma 9-55 zona 10, 4to nivel, Oficina 408, Edificio Reforma Diez
PBX-22011400, TELEFAX: 22011401



La redacción considero que se apega a lo establecido en las reglas de la Real Academia Española.

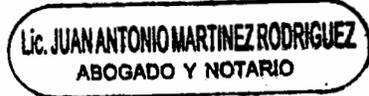
Las conclusiones y recomendaciones son acertadas respecto al desarrollo del tema, la bibliografía es la adecuada en virtud que cada uno de los autores presenta el contenido necesario y funcional para el tipo de trabajo presentado en la investigación.

En fin, dicho trabajo es satisfactorio llenando los requisitos que exige el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, razón por la cual emito **DICTAMEN FAVORABLE** a efecto de que continúe su trámite correspondiente.

Sin otro particular, patentizo al señor Jefe de la Unidad, las muestras de mi alta consideración.

Atentamente,

Juan Antonio Martínez Rodríguez
Asesor de Tesis
Colegiado 4,803



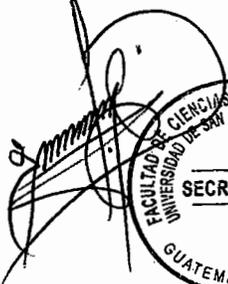


DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, 04 de agosto de 2014.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis de la estudiante JENNIFFER QUETZALI JUÁREZ VALENZUELA, titulado ANÁLISIS JURÍDICO SOBRE LA NECESIDAD DE REGULAR LA PROTECCIÓN DE DATOS PERSONALES EN EL COMERCIO ELECTRÓNICO. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.



BAMO/srrs.


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


 FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
 DECANATO
 UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
 GUATEMALA, C. A.





DEDICATORIA

- A DIOS:** Por haberme dado la vida, paciencia, fortaleza y sabiduría para alcanzar esta meta.
- A MI MAMÁ:** Gilda Marina Valenzuela de Juárez, por su amor fundamental en mi vida, gracias por su apoyo, comprensión y cuidados.
- A MI PAPÁ:** Luis Joaquin Juárez Alvarado, por su apoyo, por su ayuda sin la cual no hubiera podido lograr esta meta, por su amor incondicional, por ser mi guía.
- A MIS ABUELOS:** Por su cariño, bendiciones, estar siempre al pendiente y sobre todo por darme a los mejores papás.
- A MI HERMANA:** Ana Luisa Juárez Valenzuela, por ser mi mejor amiga, compañera en todo este proceso y por levantarme el ánimo cuando creí perderlo.
- A MI HERMANA:** Claudia Marina Milian Pinelo, por estar al pendiente, por su cariño y ánimos.
- A MIS SOBRINOS:** Carlos Enrique, Carlos Eduardo y Natali por la alegría que le han dado a mi vida y su cariño.
- A MI NOVIO Y AMIGOS:** Por ser parte de mi vida y contribuir a lograr esta meta.
- A:** La Universidad de San Carlos de Guatemala, en especial a la Facultad de Ciencias Jurídicas y Sociales.



ÍNDICE

Pág.

Introducción	i
--------------------	---

CAPÍTULO I

1. Derecho e informática.....	1
1.1. La ciencia del derecho.....	1
1.2. La informática y el derecho.....	2
1.3. El derecho informático	4
1.4. Un derecho autónomo	4
1.5. Derecho informático y derecho constitucional	5
1.6. Protección jurídica del software y bases de datos	6
1.6.1. Protección jurídica del software	6
1.6.2. Protección jurídica a las bases de datos	10
1.7. Contratos informáticos y protección del consumidor.....	12
1.8. Comercio y contratación electrónica.....	15
1.8.1. Ventajas del comercio electrónico	17
1.8.2. Desventajas del comercio electrónico.....	19
1.8.3. Validez de los contratos electrónicos	21
1.8.4. Identificación de las partes	23
1.8.5. Tiempo y lugar de perfección del contrato	24
1.9. Delito informático	26
1.10. Responsabilidad civil	28
1.11. El peligro de las nuevas tecnologías... ..	29

CAPÍTULO II

2. La protección jurídica a las bases de datos.....	31
2.1. Protección sui generis de las bases de datos	32
2.2. Argumentos a favor y en contra	33

2.3. Características del sistema de protección especial	39
2.3.1. Criterios de protección	39
2.3.2. Alcance de la protección	41
2.3.3. Derechos del titular de la base de datos	42
2.3.4. Titulares de la protección	42
2.3.5. Límites de la protección	43
2.3.6. Duración de la protección.....	43
2.4. Situación actual en el ámbito internacional	46
2.4.1. Organización Mundial de la Propiedad Intelectual	46
2.4.2. Primeras discusiones respecto de la protección sui generis a las bases de datos	48
2.4.3. Reunión de información sobre la propiedad intelectual en materia de bases de datos	51
2.4.4. Sesiones del Comité Permanente de Derechos de Autor y Derechos Conexos	52

CAPÍTULO III

3. La protección de datos personales y la información comercial.....	57
3.1. Protección de datos en América Latina	57
3.2. Privacidad y protección de datos	60
3.2.1. El concepto	60
3.2.2. El problema de la tutela del derecho a la intimidad	61
3.2.3. Principios generales, garantías y excepciones	62
3.2.4. Protección de datos: sistema norteamericano, europeo y latinoamericano	66
3.3. Seguridad de la información	67
3.4. Protección de datos en la Internet, ley aplicable y estándares internacionales .	69
3.4.1. Sociedad vigilada	70

3.4.2. Privacidad en la Internet	71
3.4.3. Menores y la Internet.....	71
3.4.4. Prevención y reacción ante las quiebras de seguridad	72
3.4.5. Privacidad en el entorno laboral.....	72
3.4.6. La privacidad ante las nuevas técnicas publicitarias.....	73
3.4.7. Privacidad y responsabilidad empresarial.....	73
3.4.8. Periodismo ciudadano.....	74
3.5. El derecho a la intimidad y la protección de datos personales.	74
3.6. El derecho fundamental a la protección de datos personales.	76

CAPÍTULO IV

4. Exposición de datos personales	79
4.1. La comercialización informal de los datos personales.....	81
4.2. Consecuencias de la revelación de datos personales.....	84
4.3. Análisis jurídico de la protección de datos personales y su comercialización.....	85
CONCLUSIONES	91
RECOMENDACIONES	93
BIBLIOGRAFÍA	95



INTRODUCCIÓN

El tema de investigación se eligió debido al desarrollo de las tecnologías de la información y comunicación; que de alguna manera impactan enormemente en todos los ámbitos de la vida actual y futura; principalmente en lo concerniente a los datos personales comercializados electrónicamente, pues son utilizados para infinidad de situaciones sin respetar el derecho a la intimidad de las personas.

Las bases de datos consisten en la organización sistemática, total o parcial de grupos de información, con miras a su explotación por uno o más sistemas de procesamiento de datos, los cuales se coordinan y ordenan de forma que se pueda acceder a ellos sin dificultad por quien conoce su ubicación o ser elegidos y revisados por quien busca información; son de gran provecho para los habitantes de una sociedad, teniendo en cuenta la gran cantidad de información que se puede consultar o bien, los usos que se le pueden dar a la misma en el comercio electrónico.

Se comprobó la hipótesis, al determinarse que en Guatemala se carece de instrumentos de protección a los datos personales en el comercio electrónico, que prohíban la comercialización de los datos mismos, lo cual provoca incertidumbre y desestabiliza al estado de derecho y el derecho a la intimidad misma.

Los objetivos logrados con el análisis fueron evidenciar las lagunas jurídicas existentes relacionadas con el comercio electrónico, plantear líneas de acción viables que permitan promover este tipo de transacciones comerciales y evitar algunos de sus efectos contraproducentes para los consumidores, la seguridad y la protección de datos; así como se exploró la experiencia jurídica comparada en materia de atención a los aspectos formales y tecnológicos del comercio electrónico, con el fin de diseñar una



línea modelo de atención a la problemática de la protección de datos.

La tesis contiene cuatro capítulos distribuidos de la siguiente manera: el capítulo primero, desarrolla los aspectos fundamentales del derecho y la informática; el capítulo segundo, desarrolla la protección jurídica de las bases de datos y su desarrollo dentro del derecho; el capítulo tercero, delimita la protección de datos personales y la información comercial como aspectos fundamentales de la investigación; y en el capítulo cuarto se determina la exposición de los datos personales, su comercialización informal, las consecuencias de esta actividad y la violación a la intimidad personal de los individuos.

Para investigar se aplicaron los siguientes métodos, el deductivo, para determinar las características de los datos personales y las condiciones necesarias para la comercialización de estos; el analítico, con el que se analizaron los elementos de los datos personales para determinar su protección y comercialización; en cuanto a la técnica de investigación se utilizó el fichaje, registrando de esta manera la información recopilada para mantener un manejo práctico y equilibrado.

Finalmente, se llegó a la conclusión de que se necesita un mecanismo de seguridad personal para poder limitar la comercialización de los datos catalogados como sensibles dentro del mundo informático; de ahí la importancia de crear algún instrumento jurídico que regule el uso, comercialización, protección y sanciones por el uso indebido de datos personales.



CAPÍTULO I

1. Derecho e informática

1.1. La ciencia del derecho

El derecho es vital para la vida ordenada en sociedad. El derecho cumple con su función de control social al limitar el actuar de la sociedad y del Estado; protegiéndolos el uno del otro, ya que cuenta con normas que regulan el actuar del Estado a fin de que no se exceda en las potestades y poder que posee para así evitar el despotismo; por otro lado, vela por el debido actuar de la sociedad dentro del ordenamiento jurídico preestablecido; teniendo la facultad de sancionar las conductas que violenten este ordenamiento para así evitar la anarquía.

La ley tiene la finalidad suprema de controlar la anarquía y el despotismo. A todos los ciudadanos les confiere derechos y les impone obligaciones. El derecho busca el equilibrio de la existencia social, por ello es importante que la ciencia del derecho se expanda y evolucione con las nuevas tecnologías que afectan la vida en sociedad entre las personas mismas y que también involucran al Estado en un campo nuevo y desconocido. La ciencia del derecho debe ser reforzada con nuevas normativas que se apliquen a la informática para así ampliar su eficacia y su ámbito; además de traspasar todas aquellas fronteras geográficas o tecnológicas.



1.2. La informática y el derecho

El internet y las nuevas tecnologías informáticas han sido fuente de revolución en todo el mundo; una revolución trascendental en la transmisión de información instantánea, tanto en tiempo como en lugar ya se ha logrado una conexión en los cinco continentes que nunca antes había existido. Este nuevo fenómeno necesita ser reglamentado por leyes de obligatorio cumplimiento; para evitar encauzar los beneficios de las nuevas tecnologías en prácticas poco provechosas y dañosas para el ser humano; con base en esto, se puede acordar un desarrollo y uso equitativo y sin perjuicio de las nuevas tecnologías para todos los países y sus habitantes.

Además de la nueva y creciente necesidad de que el uso del internet se sujete a normas jurídicas reconocidas en diversos foros internacionales; los fenómenos que se produjeron a causa de la evolución en la informática, brindaron a las personas nuevas formas de comunicación, de comercio, entre otras situaciones que no pueden ser ignoradas por el derecho; ya que éste como anteriormente indiqué es, el mediador, el encargado del control social en un Estado.

Esta tecnología progresiva en que están inmersas todas las personas, algunas inconscientes de ello, está sustituyendo poco a poco los medios convencionales de comunicación conocidos anteriormente. Actualmente, las personas pueden utilizar el internet para realizar transacciones bancarias, compra y venta de bienes, ofrecer servicios, entre otros usos que ya se han vuelto comunes entre la sociedad. Estos usos

que se le dan a la tecnología facilitan la comunicación al mismo tiempo que la hacen mucho más eficiente por su rapidez. Para la ciencia del derecho es importante poner énfasis en mantenerse de la mano en el desarrollo de las nuevas tecnologías; que destinadas al uso de la población mundial tarde o temprano siempre tendrán repercusiones en el derecho.

Los negocios electrónicos son cada vez más y no dejan de aparecer nuevos, por ejemplo: la contratación electrónica y la transferencia electrónica de fondos monetarios. Ante esto no se puede negar que se está frente a negocios jurídicos y estos cada vez están más dependientes de los nuevos sistemas informáticos; por lo que fácilmente pueden ser vulnerados al estar poco o nada protegidos jurídicamente.

“El desarrollo del comercio electrónico en internet plantea problemas desde el punto de vista legal, que podrían clasificarse así:

1. Jurisdicción competente a la hora de resolver los conflictos derivados de contratos electrónicos.
2. Legislación aplicable a tales contratos;
3. Lugar, tiempo y forma de aplicación de los contratos, que deben ser estudiados a la luz de las normas del derecho internacional privado y tratados internacionales que sean de aplicación, como el Convenio de Bruselas de 1968 y el Convenio de Roma de 1980.”¹

¹ Barrera López, Horacio Mauricio. **El derecho informático en la currícula universitaria**. Pág. 34.

1.3. El derecho informático

Se puede definir el derecho informático, derecho de internet o informática jurídica como: El conjunto de doctrinas, principios y normas jurídicas que estudian las modernas tecnologías de la información, los derechos y obligaciones que nacen de la utilización de la computadora, el internet y el ciberespacio, en busca de la protección de sus usuarios en particular y de la humanidad en general.

La informática no es ajena al derecho, aunque en algunas ocasiones parezca estarlo o quererlo y por ello, en las relaciones sociales y económicas generadas como consecuencia del desarrollo e introducción en todas las áreas y actividades de las modernas tecnologías de información y las comunicaciones; surgen los problemas de cómo resolver determinados conflictos nacidos de esa relación.

Así se encuentra por ejemplo, la necesidad de una relación jurídica de los derechos y obligaciones consecuentes de la creación, distribución, explotación o utilización del hardware y software; con su protección de los derechos de propiedad intelectual.

1.4. Un derecho autónomo

En el derecho diversas discusiones han tenido los tratadistas al determinar si una rama del derecho es autónoma o no; es decir, si se desarrolla con sus propios métodos e instituciones.

En el caso del derecho informático, no es la excepción pues ha sido objeto de diversas discusiones en busca de determinar si es un derecho autónomo o no; estas discusiones se han realizado en muchos países, lo cual muestra la importancia que se le ha otorgado al derecho informático.

“A lo largo de los debates, las investigaciones y disertaciones de prestigiosos juristas se ha concluido que la informática debe ser regulada en toda su implicación social por el derecho, el derecho informático. A pesar de esto se reconoce que el derecho informático o derecho de internet no constituye hasta ahora una nueva rama del derecho, debido a que sus conceptos e instrumentos ya son objeto de las disciplinas jurídicas existentes con anterioridad.”²

1.5. Derecho informático y derecho constitucional

El derecho informático está relacionado con el derecho constitucional, pues debe dar atención prioritaria a la protección de los datos personales; a los derechos individuales, entre ellos el derecho a la intimidad.

La protección de los datos personales y el derecho a la privacidad están amparados por figuras jurídicas como los derechos humanos, los derechos personales, los derechos patrimoniales, las libertades públicas y privadas, el derecho de la privacidad, el derecho a la intimidad y al honor de las personas, las garantías individuales y

² **Ibid.** Pág 40.



sociales.

En algunos países no existe una legislación adecuada para la protección de los datos personales; por lo que son necesarias leyes que tiendan a proteger la información de las personas, la libertad de gozar de dicha información y de regular el abuso que pueda ocurrir, menoscabando los intereses de las personas.

1.6. Protección jurídica del software y bases de datos

Con la constante evolución de los sistemas de comunicación se ha aceptado el uso de estos en todos los aspectos de la vida cotidiana; por lo que es casi inexistente una actividad comercial, profesional o personal que esté ajena a estos. Como ya mencioné, de estos nuevos usos que se le han dado a la tecnología han nacido diversas relaciones y vinculaciones anteriormente desconocidas.

1.6.1. Protección jurídica del software

Hablar de software se refiere al soporte lógico de un sistema informático, es decir, el conjunto de los componentes necesarios que hacen posible la realización de tareas específicas. El software incluye, entre muchos otros, las aplicaciones informáticas; tales como el procesador de texto, que permite al usuario realizar todas las tareas concernientes a la edición de textos; el llamado software de sistema, tal como el sistema operativo, que básicamente permite al resto de los programas funcionar

adecuadamente, facilitando también la interacción entre los componentes físicos y el resto de las aplicaciones.

“En el orden internacional se presentan algunos inconvenientes en cuanto a la protección jurídica de obras de software: cuando la Asociación Internacional para la Protección de la Propiedad Industrial (A.I.P.P.I.) se reunió en la ciudad de San Francisco (USA) en 1975, el tema de la protección jurídica del software, fue objeto de un particularizado examen, produciéndose informes sobre la situación legislativa y práctica que existen en los diversos países y las precauciones a tomar en el futuro.

Así fue como se examinaron tres modos de protección concebibles para la obra de software a saber:

- a) Patentes de invención.
- b) Derecho de autor.
- c) Sistema propio o sui generis.

Ninguno de ellos ha sido totalmente descartado hasta la fecha, pudiendo afirmarse que la triple alternativa subsiste al día de hoy; pero la mayoría de los informes y opiniones estaban y están a favor de la protección legal del software bajo el régimen legal del derecho de autor.”³

³ Campos, Celin. **El software, la propiedad intelectual y el Decreto 165/94**. Pág. 2.



a) Patentes

Con respecto a las mismas, debe indicarse que el obstáculo que rige contra la protección del software como un invento patentable; radica en que un programa es visto como una concepción puramente mental de pasos y operaciones que se instruyen hacer a un ordenador; lo cual, al no involucrar la manipulación de materia, que algunos consideran como parte esencial de un invento patentable, relegaría al programa a un terreno especulativo, ajeno al ámbito de los avances técnicos industriales que se acogen a la protección de patentes.

b) Derecho de autor

El derecho de autor no ofrece oposición en cuanto a dar cabida al software, ya que generalmente los organismos administrativos no se oponen a ello o porque existen pronunciamientos judiciales donde se sancionó la reproducción no autorizada de programas por aplicación de la legislación sobre derechos de autor. Estos fallos judiciales se fundamentaron en que la palabra software está relacionada de manera directa con el intelecto humano; indico porqué: el software es el componente intangible de un sistema informático (a diferencia del hardware que es la parte tangible) y depende necesariamente de un acto interno, del acto de un ser humano, que luego de distintas etapas de desarrollo, se exterioriza con su creación.

De esta manera esa exteriorización de pensamiento puede ser considerada como



un producto intelectual, pues es el resultado de una actividad mental de su autor, quien desarrolla, mediante la aplicación de la inteligencia, ideas, conceptos y expresiones que adquieren realidad de por sí y que generalmente se exteriorizan en la materia que le da sustento. Ahora bien, cuando estos productos intelectuales están protegidos se convierten en propiedad o derecho intelectual.

De esta manera el software, en cualquiera de sus expresiones no es algo que se encuentra en la naturaleza, sino que su sustancia depende de la inteligencia y del esfuerzo del hombre; es decir, de un acto que lo exteriorice y le dé forma.

c) Sistema propio o sui generis

En el terreno de las regulaciones sui generis, existe un significativo aporte materializado en las disposiciones tipo para la protección del soporte lógico, preparadas por la Oficina Internacional de la Organización Mundial de la Propiedad Intelectual (O.M.P.I.); luego de consultas, a nivel internacional, la mayoría de los países se adhirieron al proyecto. En él se adopta un régimen más próximo al de la propiedad intelectual que al de patentes de invención, pero con la sensible ventaja de no hacer convivir bajo una sola ley la propiedad intelectual tradicional y los particulares derechos de los creadores de software.



1.6.2. Protección jurídica a las bases de datos

Para desarrollar este tema es necesario desglosar algunos términos básicos antes, como por ejemplo, el dato es una referencia que llega a ser un elemento aislado descriptivo que no logra tener carácter de información, pues para que se transforme en ella requiere de interconexión de esos datos, de manera que vinculados se conviertan en una referencia concreta. De esta definición se deduce que el dato por si solo no constituye un peligro, es insignificante, pero el daño es generado cuando de dato en dato se empiezan a elaborar perfiles de información sobre una persona determinada, perfiles que son recopilados con información brindada por ella misma y, en otras ocasiones, obtenida sin su consentimiento.

Las bases de datos son utilizadas para almacenar infinidad de datos e información referente a cualquier situación en particular y por cualquier medio de recolección; la cual es recolectada, agrupada y clasificada, según el fin que se persiga.

En los últimos años con el continuo progreso de la informática, estas bases de datos han proliferado generando serios problemas por la recolección de datos sin consentimiento de las personas.

Para efectos de estudio expondré la siguiente clasificación de bases de datos:

“1. Base de datos referenciales: son aquellas que ofrecen registros que a su vez son

representaciones de documentos primarios. Se subdividen en:

- a) Bibliográficas: cuyo contenido son de tipo bibliográfico; y
 - b) Directorios: aquellas cuyo contenido está referido a la descripción de otros recursos de información, como por ejemplo, un directorio de base de datos.
2. Base de datos fuentes: son aquellos que ofrecen el documento completo, no una representación del mismo. Se dividen en:
- a) Numéricas: la información es de tipo numérico, como un censo o indicadores cuantitativos.
 - b) Textuales: ofrecen el texto completo del documento.
 - c) Mixtas: combina ambos tipos de información, un ejemplo de este subtipo lo sería un informe económico de empresas”.⁴

Ahora bien, es necesario individualizar el concepto de datos personales, que son aquellos datos que representan características específicas merecedoras de una mayor protección, al pertenecer a la esfera privada del individuo. A este tipo de datos personales también se les denomina datos sensibles y su contenido se refiere a cuestiones privadas cuyo conocimiento general puede ser generador de perjuicios. Hay que tomar en cuenta que existen recopilaciones en numerosos archivos con información como: fecha y lugar de nacimiento, domicilio, estado civil, raza, religión, inclinaciones políticas, ingresos monetarios, cuentas bancarias, historia clínica; los

⁴ Peña Ortiz, Paola. **El derecho al olvido**. Pág.66.



cuales son recopilados por diferentes entes, como los registros civiles, médicos académicos, culturales, políticos, administrativos, fiscales, bancarios, laborales y otros; los cuales actualmente pueden estar a disposición de un interesado, para diferentes fines, en forma instantánea.

El derecho informático protege a las personas de que la información contenida en las bases de datos pueda ser empleada con fines publicitarios, comerciales, fiscales o policíacos; actividades que pueden alterar los derechos fundamentales de la sociedad.

1.7. Contratos informáticos y protección del consumidor

El nuevo ambiente de comercio electrónico ha propiciado la existencia de un mercado abierto, virtual, con ventajas para el oferente como para el demandante. Junto a estas ventajas, se resalta la existencia de inconvenientes que hay que resolver, en especial lo relativo a la salvaguarda de los derechos de los destinatarios, específicamente los consumidores.

“En una compra realizada a través de internet, la protección antes de realizar la compra se refiere a la información y a la publicidad que el consumidor recibe y al respeto de su privacidad.”⁵

⁵ Chen Sui, Susan. **Déficit y oportunidades de la legislación costarricense sobre comercio electrónico.** Pág. 261.



El derecho a la información es un derecho del consumidor y un deber para los comerciantes; esto por cuanto los conocimientos técnicos del primero son nulos o escasos frente a los del proveedor. Este derecho es el principal que debe ejercer el consumidor, y debe asistirlo durante todas las fases del negocio y la contratación; incide tanto en los aspectos previos como durante el negocio mismo y después de finalizado éste.

Para la divulgación de la información de los bienes y servicios que ofrecen, las empresas la llevan a cabo por medio de sus páginas web, entre otros medios de comunicación. En esta página web despliegan la publicidad de lo que ofrecen. La publicidad es toda información susceptible de inducir a una persona a hacer una elección sobre un producto o servicio determinado.

El consumidor utiliza internet para buscar contenidos de información que le interesen, al mismo tiempo puede encontrar o le puede aparecer publicidad no deseada, contenidos ofensivos o ilegales. Esto hace necesario resolver jurídicamente el problema de la invasión de la privacidad, así como la comisión de delitos por internet (como la pornografía, el proxenetismo, venta ilegal de productos prohibidos, etc.). La publicidad en internet llega a todo el mundo, por lo que se hace necesario encontrar mecanismos para que no se viole la legislación nacional ni la de los países hacia los cuales va dirigida la publicidad. Esto debido a que los países no tienen las mismas prohibiciones. La publicidad que se hace debe ser lícita, honesta, decente y verídica. El anunciante debe identificarse, informar sobre las razones de una posible recopilación



de datos, indicar a quienes va dirigida la publicidad y respetar la confidencialidad, así como las disposiciones particulares sobre la publicidad infantil y las sensibilidades diversas del público mundial.

El aspecto de privacidad y más específicamente lo relacionado a la protección de datos personales es de gran importancia en el ambiente de comercio electrónico. Esto debido a que en cualquier transacción comercial que el consumidor realiza a través de una página web; el mecanismo mayormente utilizado es por medio de contratos de adhesión, que se basan en formularios prediseñados por el proveedor y en los cuales se solicita información personal al consumidor.

Por otro lado también, cuando el usuario accede a una página, simplemente para buscar información de algún asunto que le interese, aunque no compre nada, generalmente le piden información antes de otorgarle el permiso de ingresar a la página web

El usuario entrega información y no conoce ni es informado para qué ni cómo será utilizada. El derecho fundamental de la protección de los datos persigue garantizar a la persona un poder de control sobre cualquier tipo de dato personal, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho afectado.



1.8. Comercio y contratación electrónica

El comercio electrónico es una nueva modalidad de hacer negocios a nivel mundial que en un futuro puede convertirse en la modalidad más utilizada de hacer comercio. Esta nueva modalidad de comerciar tiene un impacto evidente en las economías y las culturas de los países.

Para las empresas que exploten completamente su potencial, el comercio electrónico ofrece la posibilidad de grandes cambios que modifican radicalmente las expectativas de los clientes y redefinen los mercados así como crean mercados completamente nuevos. Todas las empresas, incluidas las que ignoran las nuevas tecnologías, sentirán el impacto de estos cambios en el mercado y las expectativas de los clientes. Igualmente las personas se enfrentarán con nuevas formas de adquirir bienes y servicios, acceder a información e interactuar con otras personas en el mundo. Las posibilidades se han extendido y las limitaciones geográficas y de tiempo se han eliminado.

Por otro lado, las transacciones de tipo electrónico son contratos atípicos en prácticamente todos los países y esa condición hace que sea necesaria su regulación en todos los países del mundo.

“Una definición dada por la Unión Europea en su iniciativa europea de comercio electrónico, señala que el comercio electrónico “consiste en realizar transacciones



comerciales electrónicamente”. El caso más simple es realizar sólo la publicidad por internet, y el caso más completo es donde todos los pasos anteriores se hacen de forma electrónica, incluyendo el pago.”⁶

“Por otro lado, se evidencia que en el comercio electrónico participan como actores principales las empresas, los consumidores y el Estado. Así se distinguen normalmente tres tipos básicos de comercio electrónico:

- entre empresas o B2B (business to business)
- entre empresa y consumidor o B2C (business to consumers)
- entre empresa y administración o B2A (business to administrations)

Las empresas intervienen como usuarias (compradoras o vendedoras) y como proveedoras de herramientas o servicios de soporte para el comercio electrónico: proveedores de servicios de certificación de claves públicas, instituciones financieras, etc. Por su parte, las administraciones públicas, actúan como agentes reguladores y promotores del comercio electrónico y como usuarias del mismo (por ejemplo en los procedimientos de contratación pública o de compras por la administración).

En un sentido amplio, los consumidores participarían en dos formas adicionales de comercio electrónico además del B2C: por una parte, el comercio electrónico directo entre consumidores (venta directa entre particulares) y, por otra, las transacciones

⁶ Bruce, O. **Comercio electrónico y derechos del consumidor**. Pág. 160.



económicas entre ciudadano y administración (pago de prestaciones sociales, pago de impuestos, etc.).”⁷

El comercio electrónico supone una relación contractual que puede ser establecida desde diferentes técnicas de comunicación: página web, chat o videoconferencia, correo electrónico y subasta electrónica. Los contratos más numerosos perfeccionados por medio de una página web son los de compra y venta de un bien o servicio.

Se define el concepto de contrato a través de internet, como aquel contrato para cuya conclusión se ha empleado este medio moderno de comunicación, sin importar la calificación de los sujetos que lo hayan empleado (profesionales, particulares o un profesional y un consumidor), ni la normativa aplicable a cada uno de ellos. Estos tipos de contratos se basan en el documento electrónico, definido como: un conjunto de impulsos eléctricos que recaen en un soporte de computadora y que sometidos a un adecuado proceso; permiten su traducción a lenguaje natural a través de una pantalla o una impresora.

1.8.1. Ventajas del comercio electrónico

El comercio electrónico permite transacciones de compra y venta sin limitación física territorial; las empresas con un sitio web tienen oportunidad de vender a cualquier persona ubicada en cualquier parte del mundo. Así pues, se pueden encontrar muchas

⁷ Chen Sui, Susan. **Ob. Cit.** Pág. 31.



ventajas en este tipo de comercio, entre ellas están:

- Permite hacer más eficientes las actividades de cada empresa, así como establecer nuevas formas, más dinámicas, de cooperación entre empresas.
- Reduce las barreras de acceso a los mercados actuales, en especial para pequeñas empresas, y abre oportunidades de explotar mercados nuevos.
- Presencia de la empresa a nivel global.
- Aumento de la competitividad.
- Oferta de productos y servicios más personalizados.
- Cadenas de entrega más cortas o inexistentes.
- Reducción de costos y de precios.
- Oportunidad de nuevos negocios, productos y servicios.
- Para el consumidor, amplía su capacidad de acceder a prácticamente cualquier producto y de comparar ofertas; permitiéndole además convertirse en proveedor de información.



- Servicios de mejor calidad.
- Reduce o incluso elimina por completo los intermediarios, por ejemplo en la venta de productos en soporte electrónico (textos, imágenes, videos, música, programas, etc.) que se pagan y entregan directamente a través de la red.
- Superación del factor geográfico en la contratación.
- Inexistencia de horarios en la adquisición de productos y servicios.

El comercio electrónico obliga a redefinir el papel de los intermediarios entre productor y consumidor, eliminándolos en algunos casos, pero también creando la necesidad de funciones de intermediación nuevas en otros. Igualmente el comercio electrónico afecta al papel tradicional de otros actores, como las entidades financieras o los fedatarios públicos.

1.8.2. Desventajas del comercio electrónico

El comercio electrónico plantea también problemas nuevos o agudiza algunos ya existentes en el comercio tradicional; entre ellos se encuentran los siguientes:

- La validez legal de las transacciones y contratos sin papel.



- La necesidad de acuerdos internacionales que armonicen las legislaciones sobre comercio.
- El control de las transacciones internacionales, incluido el cobro de impuestos. La protección de los derechos de propiedad intelectual.
- La protección de los consumidores en cuanto a publicidad engañosa o no deseada, fraude, contenidos ilegales y uso abusivo de datos personales.
- La dificultad de encontrar información en internet, comparar ofertas y evaluar la fiabilidad del vendedor (y del comprador) en una relación electrónica.
- La seguridad de las transacciones y medios de pago electrónicos.
- La falta de estándares consolidados y la proliferación de aplicaciones y protocolos de comercio electrónico incompatibles.
- La congestión de internet y la falta de acceso de usuarios de suficiente capacidad a bajos costos. Los problemas citados tienen, en mayor o menor medida, un componente legal o regulatorio y un componente tecnológico, por lo que su solución requiere actuaciones en ambos sentidos.

Los sistemas de comercio electrónico disponibles actualmente son en general de alto



costo y reducida interoperabilidad.

1.8.3. Validez de los contratos electrónicos

La admisión de este tipo de contratos a la luz del ordenamiento jurídico vigente debe analizarse desde dos aspectos:

- a) La validez del empleo de internet en la contratación actual y la existencia y eficacia teórica del contrato concluido a través de ella.

- b) La prueba de la existencia de dicho contrato.

“Los documentos electrónicos deben tener las siguientes características para que sean eficaces, y seguros: inalterabilidad, autenticidad, durabilidad y seguridad.”⁸

El principal obstáculo para la admisibilidad y eficacia probatoria de los nuevos soportes de información se plantea con relación al carácter de permanencia que es esencial en la definición de documento. Documento es todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier tipo de relevancia jurídica.

El temor sobre la posibilidad de reinscripción o reutilización de los soportes informáticos

⁸ Tellez Valdez, Julio. **Derecho informático**. Pág 243.



disminuye su seguridad y confiabilidad. Un documento es auténtico cuando no ha sufrido alteraciones que varíen su contenido; lo que implica decir que la autenticidad está íntimamente vinculada a la inalterabilidad. Un documento será más seguro cuando más difícil sea alterarlo y sea más fácil de verificarse la alteración que podría haberse producido o reconstruir el texto originario.

Durable sería toda reproducción indeleble del original que importe una modificación irreversible del soporte. Se entiende por modificación irreversible del soporte la imposibilidad de reinscripción del mismo; por indeleble la inscripción o imagen estable en el tiempo y que no puede ser alterada por una intervención externa sin dejar huella.

Con respecto a la seguridad, se cuestiona la autenticidad de la representación. Con el desarrollo de claves de cifrado, el documento electrónico es al menos equivalente al instrumento escrito y firmado sobre soporte de papel en cuanto a seguridad.

Los documentos electrónicos poseen los mismos elementos que un documento escrito en soporte de papel: constan en un soporte material (cintas, disquetes, circuitos, chips de memoria, redes) sobre el cual se graba el documento electrónico; contienen un mensaje que está escrito con el lenguaje convencional de los dígitos binarios o bits, entidades magnéticas que los sentidos humanos no pueden percibir; están escritos en un idioma o código determinado; pueden ser atribuidos a una persona determinada en calidad de autor mediante firma digital, clave o llave electrónica.



“Desde la perspectiva internacional, el artículo 11 de la Ley Modelo sobre Comercio de la CNUDMI (1996) reconoce la validez de los contratos perfeccionados mediante los mensajes de datos. La contratación por vía Internet resulta perfectamente válida, y la utilización de este medio de comunicación está permitida siempre y cuando las partes no hayan prohibido expresamente su uso.”⁹

1.8.4. Identificación de las partes

En una relación de compra y venta por internet, se identifican dos partes y se caracteriza porque entre éstas no existe un contacto físico previo. Por un lado, se encuentra el proveedor o prestador de servicios definido como “cualquier persona física o jurídica que manifiesta a través de la red, y desde su propia página web, un conjunto de ofertas contractuales, ya sean de productos o servicios, cumpliendo todos los requisitos para poder ser calificadas como tales y no de simple publicidad.”¹⁰

Por el otro lado, se encuentra el usuario o consumidor, que es cualquier persona física o jurídica que utilice la página web del proveedor para comprar bienes o servicios; o simplemente para obtener información de las ofertas publicadas en la página.

La identificación de ambas partes es fundamental para dar por terminado el contrato o para conocer la condición de consumidor, profesional, empresa o particular que les corresponda en la relación; principalmente por la posibilidad que brinda el sistema para

⁹ Chen Sui, Susan. **Ob Cit.** Pág. 62.

¹⁰ **Ibid.**



cometer estafas, fraudes y abusos encubiertos o; para exigir reclamos posteriores por parte de los usuarios o consumidores.

1.8.5. Tiempo y lugar de perfección del contrato

El uso de instrumentos de comunicación entre partes físicamente distantes, hace necesario determinar en qué instante exacto se entiende perfeccionado el contrato, y cuál es el lugar en el que se considera concluido el contrato. “La importancia de la determinación de estos dos aspectos se debe a las siguientes razones:

- Conocer el momento en que entra en vigor el contrato que une a las partes para exigir las obligaciones instituidas por él.
- Ineficacia de los intentos extemporáneos de revocación y retirada de la oferta o retirada de la aceptación por parte de los autores.
- Ineficacia de determinadas causas de extinción de las declaraciones contractuales (ejemplo: incapacidad sobrevenida o muerte del autor de la declaración, caducidad, etc.)
- Transmisión de los riesgos de la cosa al adquirente, en aquellos casos en que el contrato que se perfeccione conlleve la transmisión de la propiedad u otro derecho real.



- Determinación exacta de la ley o norma aplicable en el tiempo a la relación contractual creada; es decir, los problemas típicos asociados a la aplicación temporal de las normas jurídicas.
- Momento determinante del inicio del cómputo de determinados plazos para el correcto ejercicio de algunos derechos o acciones.¹¹

Asimismo, resulta fundamental localizar el lugar exacto en que se entiende concluido el contrato, pues con ello se determina: La ley o norma aplicable especialmente a la relación contractual originada, así como los usos interpretativos relevantes para subsanar las ambigüedades de los contratos. Los requisitos básicos de la oferta son:

- Propósito del oferente de vincularse contractualmente con carácter definitivo.
- La oferta debe ser completa, es decir, debe contener todos los elementos esenciales del futuro contrato, de modo que con la simple aceptación del comprador el contrato sea perfecto.
- La oferta debe exteriorizarse. La exteriorización de la voluntad puede ser efectuada de forma expresa, tácita e incluso presunta, pero lo importante es que sea concluyente, en el sentido inequívoco.

¹¹ Menéndez, J.C. **El contrato vía internet**. Pág. 75.



La aceptación por su parte debe tener los siguientes requisitos:

- Que se exteriorice. La exteriorización puede ser de cualquier manera, por el principio de libertad de forma, pero en lo que se refiere al comercio electrónico, debe producirse electrónicamente.
- Que sea pura y simple, ejemplos: las compras o contratos por transacciones de crédito o los contratos de vacaciones.

“Entonces, la aceptación perfecciona el contrato. Una contratación vía internet, el perfeccionamiento del contrato será en el momento en que el comprador pulse el botón “aceptar”, puesto que en segundos la aceptación habrá llegado a conocimiento del oferente o a su ordenador.”¹²

1.9. Delito informático

La rápida evolución de la informática ha dado lugar al apareamiento de delitos nuevos, los llamados delitos informáticos.

Se considera que un delito informático es cualquier comportamiento ilegal en el que está involucrada una computadora. También se habla de actitudes ilícitas en que se tiene a la computadora como instrumento; como los casos del uso indebido del

¹² Pinochet R. **Contratos electrónicos y defensa del consumidor**. Pág. 112.



software, la apropiación indebida de datos o, la interferencia en sistemas de datos ajenos.

Se pueden identificar los siguientes como aquellos cuya comisión ha sido facilitada por el comercio electrónico:

- a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
- b) Lectura, sustracción o copiado de información confidencial.
- c) Modificación de datos tanto en la entrada como en la salida.
- d) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria.
- e) Intervención en las líneas de comunicación de datos o teleproceso.
- f) Interceptación de e-mail: lectura de un mensaje electrónico ajeno.
- g) Estafas electrónicas: por medio de compras realizadas haciendo uso de la red.
- h) Transferencias de fondos: engaños en la realización de este tipo de transacciones.
- i) Uso indebido de información confidencial para beneficio propio: la red facilita la obtención de datos que pueden ser mal utilizados por el proveedor.
- j) Pornografía y proxenetismo: La red facilita este tipo de comercio y hace más difícil la ubicación e identificación del proveedor.

Todos estos delitos se reducen a la problemática de la privacidad y seguridad de las transacciones electrónicas; a excepción del último, pornografía y proxenetismo, que más bien ha encontrado en la red un medio que ha facilitado su comercio.



Generalmente, los supuestos delincuentes informáticos pueden encontrarse entre algunos operadores, programadores, analistas de sistemas, analistas de comunicaciones, supervisores, ingenieros en sistemas o funcionarios superiores. Víctimas de la delincuencia informática, según numerosos casos reportados por la prensa internacional, pueden ser empresas e instituciones, tales como bancos, compañías financieras, aseguradoras, universidades y entes estatales.

En Guatemala el Código Penal, Decreto 17-73 del Congreso de la República de Guatemala, regula el delito informático en el título VI, capítulo VII: “De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos”, Artículos 274 “A” al 274”G”, contenidos en el Decreto 33-96 del Congreso de la República.

Además, cabe resaltar que el problema de la privacidad al fin y al cabo también se reduce a un problema de seguridad de la información. Por tanto, no es posible abordar sólo el aspecto de la privacidad sin analizar al mismo tiempo los asuntos de seguridad de las transacciones.

1.10. Responsabilidad civil

Como anteriormente fue indicado, el desarrollo de la tecnología y el uso constante y cotidiano de la misma por las personas individuales así como por grandes empresas; ha ido creando una dependencia a estos sistemas informáticos de comunicación y de negocios que son vulnerables debido a la poca seguridad que se les ofrece.



Cada día las grandes corporaciones basan en mayor medida su gestión en una información exacta, completa y obtenida a tiempo; por lo que es creciente la importancia de su seguridad y de su confidencialidad.

De aquí surge la importancia de mencionar la responsabilidad civil, que debe ser tema de atención por parte del estudioso del derecho; ya que con la creación de los delitos informáticos tienen en sus manos nuevas cuestiones que no están del todo previstas en el ordenamiento jurídico actual. Es importante agregar que los juzgadores ahora tendrán controversias que no se les habían presentado antes; como por ejemplo las nacidas del comercio electrónico, contratación electrónica, propiedad intelectual, protección del consumidor, todos estos conflictos surgidos por el uso del internet.

1.11. El peligro de las nuevas tecnologías

Los juristas conforme la realidad económica y social de su país y del mundo entero va cambiando deben ir investigando y poniéndose a la vanguardia de las nuevas formas de comercio, de las nuevas formas de comunicación e interacción social; para poder efectivamente normar todos los actos del ser humano que pueden tener incidencia en el derecho.

Las ventajas en el comercio que ha proporcionada la tecnología son positivas y favorecen la actividad creativa del hombre; pero hay muchos actos que infortunadamente se han encauzado para hacer daño a las demás personas. Hay que



tener en cuenta que según diversos tratadistas las nuevas tecnologías llevan consigo ventajas y beneficios para el ser humano; pero a la vez también conllevan un potencial peligro que surge del desconocimiento del alcance y uso de estas nuevas tecnologías.

Por tanto, al estar frente a un cambio y evolución en todas las áreas del derecho producto de la inclusión de la tecnología en las mismas; surge el gran debate de la jurisdicción en internet que no existe y tampoco existe regulación legal plenamente reconocida internacionalmente; por lo que queda mucho por investigar por parte de los juristas, además de mantenerse al tanto de los avances para no obviar temas importantes que afectan a todos, parezca o no.



CAPÍTULO II

2. La protección jurídica a las bases de datos

La globalización es un fenómeno mediante el cual un país que pretenda desarrollarse debe estar económica y políticamente interconectado con otros; fenómeno que se traslada a los habitantes, quienes buscan mejorar su situación y por tanto buscan la mayor interacción posible con su comunidad y la de otros países; en la cual el intercambio de datos juega un papel fundamental. Una persona que busque ser aceptada socialmente no puede quedar aislada del resto de su comunidad; en este rubro el avance de la tecnología y la creación de enormes bancos de datos públicos y privados ha generado que un desconocido deje de serlo en cuestión de minutos; lo cual implica el beneficio de la interrelación económica política y social.

Como se ve actualmente la informática es indispensable para el desarrollo de la actividad social; hoy día se facilita reiteradamente información personal a terceros, la cual se procesa con la finalidad de utilizarla en forma más eficiente; lo cual representa un importante avance, ya que mediante la utilización de las computadoras se puede procesar un enorme cúmulo de información, con lo cual la atención del solicitante de algún servicio puede demorar sólo minutos.

Sin embargo, es importante destacar que este proceso debe realizarse con el consentimiento de la persona y sólo en relación con el fin para el que le fueron



requeridos los datos; es decir, la solicitud de un crédito, una compra, una reservación, etc. En la mayoría de los casos la persona no autoriza que los datos que se le solicitan sean relacionados con otras fuentes de información; ya que por este medio se pueden obtener informes más fidedignos de su comportamiento crediticio o de otras características sociales; lo cual desde luego representa una información sumamente personal. No obstante, no contar con autorización para correlacionar bases de datos en Guatemala es una práctica recurrente. Esta forma de invasión a la privacidad mediante nuevas estrategias comerciales está proliferando considerablemente.

La protección de datos personales no aparece como consecuencia del avance tecnológico; ya que ésta se tutela desde la Declaración de los Derechos del Hombre de 1789; no obstante, regímenes autoritarios en distintas épocas se encargaron de borrar este derecho fundamental; regímenes en los que las clases dominadas no tuvieron el menor derecho sobre sus propia persona por lo que su intimidad y por tanto sus datos personales no existían. Lo que el avance de la tecnología ha hecho es generar la posibilidad de una intromisión cada vez mayor en la vida privada de las personas; intromisión que debe ser regulada y limitada.

2.1. Protección sui generis de las bases de datos

En el capítulo anterior se trató de manera general el tema de las diversas protecciones que se les otorgan a las bases de datos, entre ellas las que otorgan los derechos de autor; pero estos no abarcan a todas las bases que existen y las que pueden llegar a



existir en el futuro; esto debido a los criterios que se utilizan en este régimen. protección que otorgan los derechos de autor deja por fuera muchas bases de datos por su contenido; en especial por el gran volumen de información almacenada. Por tal razón, es necesario crear un sistema de protección específico para este tipo de obras.

Antes de analizar las características especiales que debería tener un sistema de protección especial para las bases de datos; es necesario analizar los argumentos a favor y en contra del mismo.

2.2. Argumentos a favor y en contra

Existen diversos argumentos que apoyan la creación de un sistema jurídico de protección especial para las bases de datos diferente al de los derechos de autor. “Uno de los requisitos esenciales que debe poseer una obra para obtener la protección del régimen general es la originalidad, es decir, que la obra sea creativa e individualizada por mínima que sea la diferencia, basta que no sea copia de otra, que posea un esfuerzo intelectual de características propias y que haya sido producida con el esfuerzo particular del autor.”¹³

En el caso de las bases de datos esos requisitos son difíciles de cumplir, ya que los derechos de autor exigen los requisitos anteriormente descritos, pero al tratarse de las bases de datos estos datos en sí mismos no pueden tener originalidad de ningún tipo.

¹³ Dirección Nacional del Derecho de Autor. **Génesis y evolución del derecho de autor**. Pág. 75.



Esto último es debido a que si se trata de una recopilación de datos que son parte de otras obras protegidas, ya gozan de la protección de los derechos de autor y si no se trata de este tipo de datos no será posible que el derecho de autor proteja independientemente cada dato contenido en la base de datos.

Desde otro punto de vista, muchas de las bases de datos que no satisfacen el carácter de originales, tienen consecuencias positivas para la sociedad en general, que deberían hacer a su creador recuperar la inversión hecha, evitando que terceros utilicen parte o todo del contenido de una base de datos para beneficio propio y sin ningún tipo de contraprestación; con el fin de que los particulares tuvieran algún incentivo para realizar esta tarea.

Este tipo de incentivo tendría consecuencias positivas de diversos tipos:

- a) Impulsaría el desarrollo sostenible y la comercialización de todo tipo de bases de datos, lo cual garantizaría el progreso económico y tecnológico en la producción y recopilación de información.
- b) Fomentaría la divulgación de bases de datos culturales o de gran valor desde cualquier punto de vista.
- c) Aumentaría considerablemente la creatividad e inversión en las bases de datos.



d) La inversión continua es un factor esencial para el desarrollo y perfeccionamiento de las bases de datos.

Y desde el punto de vista de los usuarios:

a) Se garantizaría la calidad de las bases de datos producidas y alentaría la creación de las mismas.

b) Garantizaría la integridad y fiabilidad de los datos, al ofrecer un producto de calidad para obtener beneficios.

c) Garantizaría el progreso económico y tecnológico.

d) Aumentaría la oferta, permitiendo que más proveedores pongan el resultado de su actividad creativa a la disposición de un público más vasto; satisfaciendo así las necesidades del consumo informacional de una inmensa gama de grupos.

“Otro problema, aunque no directamente relacionado con la protección sui generis, pero que podría ser solucionado por este medio es el alcance que se le da al término “bases de datos”. Lo que la ciencia de la informática denomina con ese nombre no es lo mismo que lo que la ciencia de la documentación llama así y menos aún lo que ha terminado significando para el léxico jurídico internacional existente.”¹⁴

¹⁴ Heredia Quecan, César. **La protección jurídica a las bases de datos.** Pág. 27.



El adelanto tecnológico es otro punto que impulsa la consagración de un mecanismo jurídico que permita a los creadores de bases de datos evitar que su contenido sea extraído. Dentro del variado grupo de bienes y servicios que se comercian electrónicamente por medios virtuales en línea; las bases de datos constituyen un producto fuertemente demandado por ciertos sectores del público y, sin duda, uno de los que tienen más antigua presencia en el mercado virtual. Su paso al ambiente del comercio electrónico se concibe mejor teniendo en cuenta los siguientes aspectos:

- a) El volumen de datos que normalmente se maneja, que requieren amplios medios de almacenamiento y poderosas herramientas de búsqueda.
- b) La necesidad de actualización constante de la información.
- c) La preferencia de los usuarios por recibir solamente el material pertinente, sin hacerse cargo de almacenar un volumen de datos que probablemente no necesitarán explotar.

El auge de las bases de datos en medios electrónicos tiene como consecuencia negativa; que cada vez resulte más fácil que un tercero copie y reorganice el contenido de una base de datos; de tal manera que la copia sea tan diferente de la compilación original que no infrinja los derechos de autor, si es que la base llega a tener dicha protección más aún si carece de ella; todo esto teniendo en cuenta que la elaboración de una base de datos requiere una gran inversión en términos de recursos humanos,



técnicos y económicos, al tiempo que su contenido se puede copiar o se puede acceder a ellas a un costo muy inferior al necesario para crearlas independientemente; lo que tiene consecuencias graves desde el punto de vista económico y técnico.

Por otro lado, los críticos a la imposición de un sistema sui generis de protección de las bases de datos; manejan los siguientes argumentos:

- a) La protección jurídica existente hasta el momento para este tipo de obras, consistente en los derechos de autor, las normas contractuales y de competencia desleal; proveen una protección suficiente a los intereses del fabricante.
- b) Esta protección legal está reforzada por las medidas técnicas de autoprotección, como mecanismos de encriptación o de bloqueo a la descarga de información, entre otros; que permiten al fabricante evitar el copiado de los datos.
- c) No se alentaría la inversión en las bases de datos, al crear una frustración en los investigadores potenciales que desearan consultar las bases de datos existentes; retrasando el progreso de la investigación en general. Por la misma razón se obstaculizaría la actividad educativa y cultural.
- d) Se restringiría de manera innecesaria la disponibilidad de información y el flujo de la misma; frenando su índice de utilización e intercambio.



- e) La coexistencia de una protección especial y de la protección otorgada por los derechos de autor para las bases de datos; podría crear una duplicación y por ende una obstaculización al momento en que los diferentes operadores de la norma tuvieran que aplicarla.
- f) Se limitaría innecesariamente la divulgación de información con fines educativos y científicos. Además, el modelo de mercado para el acceso a los datos y la información no se adecua a la investigación científica y a la educación, las cuales son de carácter cooperativo, completamente opuesto al carácter competitivo de la empresa privada; en especial porque ninguna entidad de manera individual divulgaría todos los datos necesarios para adelantar de manera efectiva este tipo de actividades. Por otra parte, el costo de la investigación científica se elevaría, disminuyendo la velocidad y las posibilidades de éxito.
- g) El mercado en el cual se puede ofrecer una base de datos como producto o el ingreso a ella como servicio; resulta muy pequeño comparado con los altos costos de inversión que son necesarios para recopilar un producto y servicio atractivo para los usuarios y; por lo tanto, rentable. El hecho de crear una mayor protección no aumenta el tamaño de ese mercado.
- h) No parece pertinente promulgar un nuevo tipo de protección, socialmente costoso como solución a un problema cuya existencia no ha sido comprobada. Pero en caso de comprobarse la deficiente protección, existen otros medios socialmente más



deseables, que pueden ser encontrados en legislaciones.

2.3. Características del sistema de protección especial

2.3.1. Criterios de protección

Esta es una de las características más importantes en que se debe inspirar el sistema sui generis de protección; ya que se refiere al equilibrio que debe existir entre el proteger la inversión del productor de bases de datos frente a la competencia comercial desleal; así como frente a la necesidad de asegurar la libre circulación de los datos al servicio de la investigación científica; además de satisfacer las exigencias de la vida social.

Para lograr estos cometidos, es necesario que se creen criterios que permitan distinguir qué bases de datos tendrán protección especial, tratando de abarcar la mayor cantidad posible pero bajo estrictos estándares; que dejen fuera a las que no merecen la protección. Esta es una gran diferencia con el sistema de los derechos de autor, ya que éste no evalúa extensivamente las obras para ser objeto de protección. Esta diferencia nace porque los dos sistemas persiguen distintos fines, pues el derecho de autor protege la expresión del creador, sin que interese la utilización de la obra, mantiene los derechos morales sobre los económicos; mientras que la utilización de las bases de datos le da más relevancia a los derechos de tipo económico.



“Otro punto importante de mencionar es que entre los criterios que se deben tener para otorgarle o no protección a las bases de datos es poner atención en la naturaleza de las creaciones; es decir ampliar la protección a aquellas bases de datos que se encuentran en medios electrónicos, como las que no lo están.”¹⁵

Para alcanzar los objetivos descritos se ha ideado un criterio de clasificación efectivo, que consiste en otorgar protección solamente a aquellas bases de datos en las que para la obtención, verificación o selección de su contenido se hubiere necesitado una inversión sustancial; sea ésta cuantitativa o cualitativa.

“Esta inversión sustancial esencial para la producción de una base de datos puede consistir en:

- a) Recursos humanos
- b) Recursos financieros
- c) Recursos técnicos

La valoración de la importancia de la inversión debe basarse en criterios objetivos y la prueba de la “sustancialidad” debe ser de responsabilidad del titular de los derechos derivados de la protección, es decir, a quien le interesa directamente obtener la protección.

¹⁵ **ibid.** Pág. 33.

Ahora bien, el proceso de elaboración de una base de datos se compone de varias etapas bien definidas:

- a) La recopilación de la información.
- b) El ensamblaje.
- c) La verificación.
- c) La organización o presentación del contenido de la base de datos.

Las anteriores mencionadas son las más importantes etapas de la elaboración de una base de datos y en cualquiera de ellas puede presentarse una inversión sustancial que podría servir como requisito para obtener la protección sui generis.”¹⁶

2.3.2. Alcance de la protección

En cuanto a los actos contra los cuales se encamina la protección especial, se pueden clasificar en dos tipos:

- a) Todos aquellos que constituyan transferencia permanente o temporal de la totalidad o de una parte sustancial del contenido de una base de datos a otro soporte por cualquier procedimiento o bajo cualquier forma. Esta clase de actos puede ser distinguida con el término extracción, copia o reproducción por cualquier forma conocida o que sea desarrollada en el futuro.

¹⁶ **Ibid.** Pág. 33.



b) Los actos de utilización. Se refiere a la puesta a disposición del público la totalidad o de una parte sustancial del contenido de una base de datos por cualquier medio. En estos actos están comprendidos la difusión tangible como la intangible, incluida la distribución de copias materiales y todas las formas de transmisión; abarca la puesta a disposición del público de una base de datos en línea o por medios locales.

2.3.3. Derechos del titular de la base de datos

De acuerdo con todo lo anteriormente expuesto, los derechos que se crearían para el titular de los derechos sobre una base de datos; consistirían en la posibilidad de autorizar o prohibir la extracción o utilización de su contenido. La protección prevista no impide a terceros recopilar, ensamblar o compilar independientemente obras, datos o materiales de cualquier fuente distinta a una base de datos protegida.

“Estos derechos serán libremente transmisibles por causa de muerte o por acto entre vivos, al tratarse de derechos meramente económicos, razón por la cual no se encuentra ningún motivo para limitar su libre circulación.”¹⁷

2.3.4. Titulares de la protección

En cuanto a determinar quién debe ratificar los derechos derivados de la protección sui generis; se puede hacer por el fabricante o fabricantes de la base. En el último caso,

¹⁷ **ibid.** Pág. 37.



estos deberán poseer los derechos conjuntamente y la autorización de cada titular es necesaria para la extracción o utilización de una parte sustancial, al igual que para la cesión, transferencia o concesión de una licencia.

Teniendo en cuenta el carácter estrictamente económico de los derechos derivados de este tipo de protección; los mismos deben poderse transmitir por actos entre vivos o por causa de muerte.

2.3.5. Límites de la protección

Uno de los criterios de consagración legal tomados del derecho de autor, es que se debe permitir la posibilidad de consagrar excepciones a la extensión de estos derechos; pero limitándolos a ciertos casos especiales y no deben entrar en conflicto con la explotación normal de la base de datos, ni deben causar un perjuicio injustificado a los intereses legítimos del titular del derecho.

2.3.6. Duración de la protección

La duración de la protección debe ser limitada en el tiempo. En general la duración de los derechos derivados de la propiedad intelectual, depende necesariamente de muchos factores: la naturaleza del objeto protegido y los intereses de los titulares de los derechos, los usuarios y la sociedad en general. La ley específica de la materia deberá regular el tiempo de duración.



“En el caso de las bases de datos, la necesidad de una protección, en primer lugar, está ligada a la facultad de los fabricantes de bases de datos de recuperar la inversión que han realizado en una base de datos. El periodo de vida económica de las diferentes bases de datos varía según su contenido y según la estructura del mercado.

En el caso de las bases de datos dinámicas que están en constante cambio y desarrollo, se podría justificar un periodo de protección más corto. Las nuevas versiones pueden ser protegidas en virtud del tratado propuesto y las versiones antiguas se convierten rápidamente en objetos obsoletos e inútiles. En el caso de las bases de datos estáticas, tales como las bases de datos enciclopédicas, históricas y cartográficas, la protección podrá ser necesaria durante un periodo de tiempo más largo.

En realidad, si se quiere recuperar las importantes inversiones que han sido necesarias para la producción de esas bases de datos, se justifica o incluso es necesario un periodo de protección más largo. Por razones prácticas, lo recomendable sería adoptar una duración de la protección única para todos los tipos de bases de datos.”¹⁸

La duración del plazo de protección comenzaría desde el momento en que la base de datos satisfaga por primera vez los requisitos necesarios para la protección.

¹⁸ Organización Mundial de la Propiedad Intelectual. Documento CRNR/DC/6. Pág. 14.



Sin embargo, en caso de que una base de datos sea modificada de manera sustancial, por ejemplo realizando actualizaciones de su contenido; se debe entender que se convierte en una nueva base de datos con derecho a su propio plazo de protección.

Los tipos de modificaciones que entrañarán la formación de una nueva base de datos con su propio plazo de protección; son las modificaciones sustanciales en el contenido de la base de datos que constituyan una nueva inversión sustancial. Dichas modificaciones podrán resultar de la acumulación de actos sucesivos como adiciones, supresiones, verificaciones, modificaciones en la organización o en la presentación, entre otros.

Lo anterior no significa un periodo de protección ilimitado debido a la posibilidad de extender la duración de la protección cada vez que se modifique la base de datos; puesto que si se modifica considerablemente una base de datos mediante un aporte sustancial de nuevos esfuerzos, lo que resultará será una nueva base de datos; la cual debe gozar de su propio periodo de protección. Por otro lado, la versión antigua de la base de datos quedaría desprotegida al expirar el plazo inicialmente otorgado.

“Por último, siguiendo la filosofía que guía los derechos de autor, la protección no debe estar sujeta ningún requisito de tipo formal.”¹⁹

¹⁹ Heredia Quecan, César. **Ob. Cit.** Pág. 40.



2.4. Situación actual en el ámbito internacional

2.4.1. Organización Mundial de la Propiedad Intelectual

a) Historia

“Los orígenes de la Organización Mundial de la Propiedad intelectual se remontan al siglo XIX. En 1873, con ocasión de la Exposición Internacional de Invenciones de Viena, se hizo presente la necesidad de crear un sistema internacional de protección a la propiedad intelectual, puesto que varios de los expositores extranjeros se negaron a asistir por el miedo a que les robaran las ideas para explotarlas comercialmente en otros países.

En 1883 se dio un paso histórico en este sentido, pues se adoptó el Convenio de París para la Protección de la Propiedad Industrial, primer instrumento internacional que intentó dar protección a las creaciones intelectuales de los nacionales de un país en otros países. Este tratado solamente se ocupaba de las patentes, las marcas, los dibujos y los modelos industriales.

Cuando el convenio entró en vigor al año siguiente, se estableció una oficina internacional encargada de llevar a cabo las tareas administrativas como la organización y las reuniones de los Estados miembros.



En 1886 se adopta el Convenio de Berna para la Protección de las Obras Artísticas Literarias, que tenía la misma intención que el anterior, pero referido a obras creativas, especialmente de tipo artístico. También se creó una oficina internacional para administrar este documento.

En 1893 las oficinas se unieron para formar lo que se denominaría las oficinas internacionales reunidas para la protección de la propiedad intelectual, precursora de la OMPI.

Ya en el siglo XX, en 1960 las oficinas se trasladaron de Berna a Ginebra con el fin de estar más cerca de las Naciones Unidas y de otros organismos internacionales. Diez años después entró en vigor el Convenio que establece la Organización Mundial de la Propiedad Intelectual, momento en el cual las oficinas pasaron a ser parte de la OMPI. En 1974 la OMPI pasó a ser un organismo especializado del sistema de organizaciones de las Naciones Unidas con el mandato específico de ocuparse de las cuestiones relativas a la propiedad intelectual que le encomendaran los Estados miembros de este organismo.

En 1978 la secretaría de la OMPI se trasladó a Ginebra, Suiza, lugar en donde funciona actualmente.²⁰

²⁰ **Ibid.** Pág.45.



2.4.2. Primeras discusiones respecto de la protección sui generis a las bases de datos

“En el programa de la OMPI para el periodo de años de 1990-1991, se consagraron disposiciones para convocar un Comité de Expertos que se encargaría de examinar la posibilidad de redactar un protocolo al Convenio de Berna para la Protección de las Obras Literarias y Artísticas. El Comité celebró dos sesiones. En la segunda de ellas el Comité se dividió en dos diferentes, uno con la misión de continuar el estudio del protocolo mencionado y otro formado con el fin de estudiar la posibilidad de crear un instrumento para la protección de los derechos de los artistas intérpretes o ejecutantes y los productores de fonogramas.

En las sesiones de los Comités de Expertos celebradas en diciembre de 1994, la delegación de la Comisión Europea presentó un informe sobre progresos realizados en la proposición de una Directiva Comunitaria Europea sobre la protección jurídica de las bases de datos, que incluía la propuesta de creación de un derecho sui generis que se concedería al fabricante de una base de datos no original. En las sesiones de septiembre de 1995 la Comunidad Europea y sus Estados miembros presentaron a los Comités un documento de trabajo sobre el derecho sui generis previsto en la propuesta de directiva sobre la protección jurídica de las bases de datos. Después de que la delegación de la Comisión Europea hubo formulado sus comentarios al respecto, se concluyó que la cuestión de un posible sistema de ese tipo sería debatida nuevamente en las siguientes sesiones de los Comités, sobre la base de las propuestas que



pudiesen formular los diferentes países y la Comisión Europea.

En las sesiones de febrero de 1996, la Comunidad Europea y sus Estados miembros presentaron una propuesta de armonización internacional de la protección sui generis de las bases de datos; la cual incluía un proyecto de clausulado para un posible tratado sobre el tema.

Los Comités examinaron la propuesta y varias delegaciones manifestaron su interés en la protección sui generis, así como en que se continuara el estudio de este asunto.

En las sesiones de mayo de este mismo año, los Estados Unidos de América también presentaron una propuesta sobre la protección sui generis de las bases de datos junto con un proyecto de articulado para un tratado. Los Comités examinaron en conjunto las dos propuestas de tratado mencionadas.

En febrero fue convocada una conferencia diplomática de la OMPI sobre ciertas cuestiones de derecho de autor y derechos conexos para diciembre de 1996; en la cual se propuso discutir la adopción de un tratado que consagrara la protección sui generis a las bases de datos, entre otros.

El 30 de agosto de 1996, el presidente de los Comités dio a conocer el proyecto del tratado mencionado, junto con varias notas explicativas de cada uno de los artículos del tratado, fruto de las discusiones de los comités de expertos.



A pesar de todo el preámbulo descrito, en la conferencia de diciembre de 1996 no fue posible discutir el proyecto de tratado, razón por la cual expidió una recomendación instando a que se convocara una sesión extraordinaria de los órganos rectores de la OMPI competentes, durante el primer trimestre de 1997, para decidir el programa de los trabajos preparatorios para un tratado relativo a la propiedad intelectual respecto de las bases de datos.

El 20 y 21 de marzo de 1997 se celebraron los debates de los órganos rectores de la OMPI, varias delegaciones solicitaron un mayor tiempo para llevar a cabo los debates sobre el tema y los representantes de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, UNESCO, y la Organización Meteorológica Mundial, OMM, destacaron la importancia de tomar en consideración no solamente los intereses de los productores de bases de datos, sino también los aspectos de educación, investigación, enseñanza, ciencia, tecnología e intercambio de datos meteorológicos, así como los intereses de otras partes involucradas.

El Comité tomó sólo una decisión relativa al tema, pero de vital importancia para el mismo, que fue la convocatoria para la reunión informativa los días 17 y 18 de septiembre de ese año."²¹

²¹ **Ibid.** Pág. 47.



2.4.3. Reunión de información sobre la propiedad intelectual en materia de bases de datos

“La reunión informativa fue celebrada entre el 17 y el 18 de septiembre de 1997. Las discusiones y debates se realizaron con base en los memorandos preparados por la Oficina Internacional de la OMPI referidos a la legislación nacional y regional existente relativa a la propiedad intelectual en materia de bases de datos y a la información recibida de los Estados miembros de la OMPI y de la Comunidad Europea y sus Estados miembros respecto de la propiedad intelectual en materia de bases de datos.

La reunión informativa dio como resultado una recomendación en la cual se instaba a la Oficina Internacional de la OMPI a elaborar un documento que resumiera las cuestiones planteadas durante dicha reunión. En este documento se debía invitar a los Estados miembros de la OMPI y a la Comunidad Europea, así como a las organizaciones intergubernamentales y no gubernamentales invitadas a la reunión de información, a que presentaran, a más tardar a finales de abril de 1998, información relativa a las cuestiones incluidas en el documento mencionado, así como cualquier otra cuestión relacionada que consideraran pertinente.”²²

²² **Ibid.** Pág. 51.



2.4.4. Sesiones del Comité Permanente de Derechos de Autor y Derechos

Conexos

“Del 2 al 10 de noviembre de 1998 se llevaron a cabo las primeras sesiones del Comité Permanente, en las cuales se adelantó una discusión y un debate sobre el tema de la protección sui generis a los derechos de autor. Se invitó a los representantes de todos los Estados miembros y de las demás entidades invitadas a participar de la discusión. En el transcurso de las investigaciones se hizo evidente que no existía un consenso mundial sobre los beneficios de un sistema de protección sui generis de las bases de datos. Mientras que algunas de las delegaciones apoyaron la creación de una protección de este tipo a nivel mundial concordando con la posición de la delegación de la Comunidad Europea, otros manifestaron su preocupación respecto a este tipo de regulación.

La segunda sesión del Comité fue llevada a cabo en Ginebra del 4 al 11 de mayo de 1999. En general, las delegaciones mantuvieron sus posiciones. Como intervenciones novedosas se pueden destacar la de la República Centroafricana que expuso la existencia de la protección a las bases de datos en este país y sus resultados positivos, siempre teniendo en cuenta los intereses de los usuarios y la permisión de utilidades no comerciales; la de la delegación de México mencionó que, desde diciembre de 1996, las bases de datos originales eran objeto de protección en su país en tanto que obras derivadas, mientras que las bases de datos no originales gozaban de una protección sui generis durante un plazo de cinco años, renovable una sola vez. Hasta



ese momento, se habían registrado 60 bases de datos y la protección no había planteado problema alguno.

La reunión, además de reiterar todo lo dicho en las primeras sesiones sirvió para que varios Estados miembros expusieran a los demás sus respectivas situaciones internas y para escuchar a las organizaciones no gubernamentales que tenían intereses en este campo. No hubo un avance importante en estas sesiones, simplemente se ordenó que el tema se mantuviera en el orden del día de la tercera sesión del Comité Permanente. La tercera sesión del Comité Permanente se llevó a cabo en Ginebra del 16 al 20 de noviembre de 1999. Los resultados de esta reunión tampoco aportaron mucho al desarrollo del tema; se reiteraron las posiciones y algunos Estados miembros y entidades invitadas expusieron sus inquietudes respecto del tema; por ejemplo la monopolización de información, la flexibilidad que debía presentar una legislación de tipo internacional, el concepto claro de inversión sustancial.

El Comité Permanente recomendó en esta ocasión incluir de nuevo el tema de protección sui generis a las bases de datos en el orden del día de la próxima sesión; y actualizar la documentación relativa a la legislación vigente en relación con la protección jurídica de las bases de datos.

Para el cuarto Comité, realizado entre el 11 y el 14 de abril del 2000, no fue incluido en el orden del día de ninguna de las reuniones el tema de las bases de datos.



En el quinto Comité, celebrado entre el 7 y 11 de mayo del 2001, se incluyó de nuevo el tema. En su intervención la delegación de la Comunidad Europea recordó la protección sui generis instaurada por medio de la directiva comunitaria ya mencionada en repetidas ocasiones en este trabajo. También presentó un informe de la aplicación interna de la misma en los Estados miembros. Todos habían incluido dentro de su legislación interna las normas de la directiva y la aplicación de la misma en los tribunales y en la actividad común de los particulares había resultado del todo satisfactoria; en especial sin presentar los efectos secundarios temidos por varias delegaciones en las reuniones anteriores.

En esta ocasión todas las intervenciones estuvieron de acuerdo en que la legislación sui generis era positiva para el tráfico de la información en general; varias de las delegaciones expresaron la inclusión de una protección a las bases de datos no originales en sus legislaciones internas o; por lo menos, la existencia de proyectos de ley en los órganos legislativos de varios de ellos.

La única decisión tomada en este sentido fue ordenar que el tema de la protección a las bases de datos no originales fuera incluido en el orden del día de la siguiente sesión del Comité Permanente.

Del 26 al 30 de noviembre de 2001, se celebró la sexta y, hasta el momento, última sesión de reuniones del Comité Permanente. Se repitió la misma tendencia de las últimas dos ocasiones, todas las delegaciones y los organismos invitados intervinientes



en los debates reiteraron su posición favorable respecto de la protección sui generis de las bases de datos no originales; considerando que las consideradas originales estaban protegidas por la legislación de derecho de autor; a pesar de lo anterior, al no estar listo aún para su estudio el informe de la repercusión de una protección de este tipo para países en desarrollo; se aplazó cualquier decisión en este sentido y se ordenó de nuevo incluir el tema en el orden del día de la siguiente sesión de reuniones; a la fecha no ha sido realizada.²³

²³ **Ibid.** Pág. 56.





CAPÍTULO III

3. La protección de datos personales y la información comercial

3.1. Protección de datos en América Latina

En materia de protección de datos en América Latina la regulación es aún débil y no ha presentado progreso significativo; esto debido a la inexistencia de una unidad regional que consecuentemente reagrupe las realidades sociales tan diversas para tener avances mayores.

Desde otro punto de vista, existen diversos factores que han perjudicado el progreso de la protección de datos en América Latina; tal como el bajo nivel del desarrollo tecnológico durante los años.

Existen en América Latina regulaciones que se pueden clasificar como constitucionales y legales por una parte, como generales y sectoriales por otro. Con mucho énfasis en derecho esencial, principios y garantías. Completa el panorama latinoamericano el prestigio ascendente de la acción de habeas data.

Existe igualmente un proceso de cooperación Europa-Latinoamérica con el estándar adoptado por Europa en materia de transferencia de datos personales a terceros países; conocido dicho proceso como flujo de datos.



En Argentina ya se ha consagrado la acción de habeas data a favor de toda persona para tomar conocimiento de sus datos y finalidad; que consiste en registros o bancos de datos públicos o privados destinados a proveer informes, y en caso de falsedad o discriminación exigir supresión, rectificación, confidencialidad, actualización; Argentina es el único país latinoamericano que goza de protección adecuada con respecto a los datos transmitidos por la Comunidad Europea.

Brasil prevé el habeas data, la protección a la intimidad y a la vida privada, así como la inviolabilidad de las comunicaciones donde se sitúan los datos.

El caso de Chile está vinculado a su Constitución Política en la cual asegura a todas las personas el respeto y protección a la vida privada y pública, y a la honra de la persona y de su familia.

En México el marco general lo da también su Constitución Política que establece el derecho de privacidad; que consiste en que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones. Además existe una ley específica que trata de la protección de datos personales; donde se establece el acceso y corrección de la información de carácter personal. Existen igualmente normas vinculadas a otros sectores de la sociedad pero en la misma materia; como la Ley de Salud Pública que regula el acceso a expedientes médicos, etc.

En Panamá no existe un precepto constitucional orientado a la protección de datos,



solamente regula la inviolabilidad de correspondencia, papeles privados y comunicaciones telefónicas.

Respecto a la legislación existente que regula la protección de los datos personales en el país; el antecedente es la Constitución Política de la República de Guatemala, que preceptúa protección a las acciones privadas, al principio 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.

La inviolabilidad de la vivienda está contenida en el Artículo 23 de la Constitución Política de la República de Guatemala; es así que la inviolabilidad de datos dentro de la vivienda también está protegida por la Carta Magna.

La inviolabilidad de correspondencia, documentos y libros se encuentra en el Artículo 24 de la Carta Magna; del cual 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 deja al descubierto la información personal que puede llegar a ser utilizada con fines ilícitos; por lo que se viola el derecho a la protección de los datos.



El Artículo 31 de la Carta Magna regula el acceso a archivos y registros estatales, de esto puede inferirse que tanto el manejo de archivos de información es un derecho pero también tiene restricciones; ya que el mal uso de este derecho podría resultar en violación de derechos o discriminación hacia las personas, de las cuales se obtienen datos como los concernientes a su afiliación política.

3.2. Privacidad y protección de datos

3.2 1. El concepto

En la actualidad ya se conocen los beneficios que brinda el internet y el comercio electrónico para mejorar la calidad de vida de las personas; al mismo tiempo se ha advertido la necesidad de crear mecanismos para proteger los derechos fundamentales de las personas que pueden ser perjudicadas por ese medio. Entre los derechos que pueden estar en riesgo por el contacto con las nuevas tecnologías están: los comúnmente llamados derechos de la personalidad.

Se define el derecho a la intimidad como el derecho a que los demás no conozcan los datos personales y; que estos datos personales estén protegidos con una serie de garantías jurídicas frente a la intromisión de los demás. Se considera idéntico el término de derecho a la intimidad con el término de derecho a la privacidad; aunque para algunos autores sean diferentes. Esto es, la privacidad abarca una esfera más amplia de las facetas de la personalidad del individuo que, aisladamente consideradas,

pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. En tanto que la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona, el domicilio, las comunicaciones en las que se expresan sus sentimientos, por ejemplo.

3.2.2. El problema de la tutela del derecho a la intimidad

El derecho a la intimidad debe ser considerado en una nueva dimensión, el de la tutela de las posibilidades de participación reales del ciudadano en una sociedad que se informatiza. Esta nueva dimensión de la intimidad debe considerar la libertad y las facultades de control que un ciudadano debe tener sobre el flujo de informaciones que circulan sobre sí mismo.

Esa intimidad se puede preservar mediante la libertad informativa, que es el derecho que tienen las personas a decidir por sí mismas cuándo y dentro de qué límites procede revelar secretos referentes a su propia vida. Este derecho, no sólo se vincula con la intimidad, sino también con derechos constitucionales como: la dignidad humana y la libertad individual.

Surge también la preocupación por determinar si las bases de datos pueden ser transferidas con propósitos comerciales; y si no existe un deber de custodiarlas a cargo de quienes las confeccionan.

En el ambiente de comercio electrónico donde la plataforma básica es el internet, los datos de los usuarios se transmiten a través de la red y muy posible traspasando fronteras entre países. Surge aquí también el problema del derecho aplicable.

En el tema de la protección de la información personal se reconoce la existencia de una serie de principios generales, garantías y excepciones; que están condicionados por el principio de equilibrio o balance. Los principios generales subyacen a toda la problemática y son esenciales para garantizar, en forma directa, la adecuada protección de la información personal (y, en algunos casos, los intereses legítimos de personas jurídicas); e indirectamente, para salvaguardar los derechos de la privacidad, al honor, a la reputación, a la libertad de expresión (incluyendo la libertad de prensa), etc., mediante la generación de un adecuado marco jurídico en donde puedan hacerse efectivos todos y cada uno de estos derechos y garantías fundamentales del hombre.

3.2.3. Principios generales, garantías y excepciones

Los principios generales responden a la siguiente enunciación y fundamentación:

- a) Legitimidad y buena fe. Es fundamental que toda información relativa a las personas sea procesada en forma legítima y no pueda ser utilizada con fines contrarios a la buena fe.

- b) Especificación de la finalidad, racionalidad y duración. El tratamiento de la información debe realizarse con fines determinados, los cuales además de ser explícitos y legítimos, deben poder asegurar que la utilización o divulgación posterior no sea incompatible con los fines originarios especificados y, si lo fueren, debe mediar consentimiento del interesado que así lo autorice. Asimismo, la racionalidad de su utilización implica que los datos deben ser utilizados sólo cuando lo justifique la finalidad para la cual fueron recolectados y no en otras circunstancias que, aunque igualmente legítimas, no fueran razonables para esos fines. Finalmente, la información no podrá ser conservada por un período de tiempo que exceda el razonablemente necesario para la consecución de los fines para los cuales fue recolectada.
- c) Pertinencia y exactitud. La información referida a las personas que esté sometida a procesamiento debe ser adecuada, pertinente y no excesiva con relación al ámbito y los fines.
- d) No discriminación. El objetivo de este principio es evitar que el tratamiento de los datos relativos a las personas pueda converger en actos ilegítimos o discriminatorios.
- e) Confidencialidad y seguridad de la información. Es fundamental que pueda garantizarse al interesado que la información que le concierne sólo será tratada por la persona autorizada. Asimismo, debe garantizarse que la información estará debidamente protegida, para lo cual deberán adoptarse las medidas técnicas



de seguridad y de organización necesarias para garantizar un adecuado resguardo de los datos.

Las garantías son la condición de operatividad de los principios, siendo las siguientes:

- a) “Derecho de acceso. Es aquél que permite a los interesados conocer las instituciones y el tipo de información que dispongan sobre su persona (quien, cómo, cuándo, para qué).”²⁴

- b) Derecho de rectificación. Complementario al anterior, dicho derecho permite solicitar al interesado una modificación en los términos de alteración o ampliación, o una supresión o cancelación de aquellos datos que, referidos a su persona, considere como inexactos o irrelevantes o que requieran actualizarse.

- “c) Derecho de oposición. El interesado tiene derecho a oponerse en cualquier momento y siempre que posea un interés legítimo basado en su situación particular al tratamiento de datos; en dos supuestos:
 - i) Cuando la oposición del interesado está basada en una causa justificada, el tratamiento que efectúe el responsable ya no podrá referirse a esos datos.

²⁴ Téllez, Julio. **Ob. Cit.** Pág 62.



ii) Cuando el responsable fuera a utilizarlos con fines de investigación.”²⁵

- d) Derecho al consentimiento y a fijar el nivel de protección. En todo procesamiento de datos se requiere que el interesado preste su consentimiento al respecto en forma inequívoca; salvo cuando exista una disposición en contrario. Mediante el derecho de libertad se otorga a la persona la posibilidad de determinar el nivel de protección que desea que se otorgue a los datos que le conciernen.
- e) Derecho de uso conforme al fin. Consiste en que el interesado pueda exigir que su información nominativa sea destinada para los objetivos específicos por los cuales se proveyeron.
- f) Derecho para la prohibición de interconexión de archivos. Que las distintas bases de datos, no puedan consultarse o vincularse indistintamente.

En relación a las excepciones a dichos derechos fundamentales en el equilibrio del Estado y su poder coercitivo y los integrantes de la sociedad; se tienen a aquéllas derivadas con motivo de la seguridad del Estado tanto en lo interno como en lo externo; así como las relativas a intereses monetarios, persecución de delitos, motivos de salud, protección del propio interesado o de los derechos y libertades de terceros, entre otros.

²⁵ Sarra, A.V. **Comercio electrónico y derecho: aspectos jurídicos de los negocios en internet.** Pág. 204.

3.2.4. Protección de datos: sistema norteamericano, europeo y latinoamericano

La Unión Europea ha avanzado hasta poner en vigencia una reglamentación sobre protección de datos. Esta reglamentación tiene por objetivo proteger a las personas objeto de tratamiento de datos por parte de órganos e instituciones de la Unión Europea. También se anunció el día 7 de diciembre de 2000 en Niza, la Carta de Derechos Fundamentales de la Unión Europea, que incluye el Artículo 8; el cual regula detalladamente aspectos relacionados con la protección de datos: “Toda persona tiene derecho a la tutela de sus datos personales. Estos datos sólo deben ser procesados de buena fe para el fin preestablecido con el consentimiento de la persona afectada o para cumplir con los fines establecidos con un adecuado fundamento legal. Toda persona tiene el derecho a recibir información sobre los datos referidos a su persona que hayan sido recogidos y a lograr su rectificación. El cumplimiento de estas reglas será vigilada por un centro independiente”.

El sistema norteamericano de protección de datos es completamente opuesto al modelo europeo. Los norteamericanos no han dictado leyes específicas en la materia, sino que han preferido un sistema de autorregulación, especialmente desde el punto de vista del consumidor; indicando que los proveedores deben divulgar sus políticas de privacidad con el fin de que los consumidores puedan escoger el que ofrezca un mejor nivel de tutela.



La posición de autorregulación de Estados Unidos ha representado un gran problema para establecer acuerdos de libre comercio con la Unión Europea. Los europeos necesitan algo más que la promesa de la autorregulación.

“Por otro lado, Latinoamérica ha recurrido al hábeas data como forma de tutela de los ciudadanos frente al tratamiento de sus datos personales, el hábeas data pretende hacer referencia a la posibilidad jurídica de proteger el derecho de los ciudadanos a acceder a las informaciones personales que se encuentren disponibles en registros magnéticos y manuales con el fin de ser revisados, y si representan para la persona un perjuicio, también el de ser corregidos o eliminados es una garantía para acudir a una determinada vía y ahí solicitar los datos o las informaciones que se entiende son lesivas a los derechos protegidos, y como pretensión solicitar la anulación, borrado, obstrucción o corrección de los datos que afectan a la persona.”²⁶

3.3. Seguridad de la información

El concepto de seguridad aplicada a la información se asocia con la disponibilidad, la seguridad física, la integridad y la confidencialidad. Los aspectos de seguridad física y disponibilidad están relacionados a vulneraciones al medio utilizado para almacenar la información o al lugar en donde se encuentra. Por ejemplo, se debe asegurar la información contra incendios o inundaciones, evitar la apropiación indebida de soportes magnéticos, que se pueda seguir trabajando cuando no hay energía eléctrica o si falla

²⁶ Chirino, A. y M. Carvajal. **El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica**. Pág. 230.

el equipo o línea de comunicación; para esto debe existir alternativo operativo.

La integridad de la información se pierde cuando se producen variaciones no autorizadas, que pueden consistir en información añadida, borrada o modificada.

La confidencialidad se cumple si los datos son sólo conocidos por las personas autorizadas. Esto es un concepto relacionado con la privacidad, como derecho de las personas a determinar qué datos suyos pueden ser conocidos, por parte de quiénes y durante cuánto tiempo. “La confidencialidad puede verse afectada, por falta de políticas generales y de una clasificación de la información (qué es de uso restringido, departamental, confidencial); ausencia de procedimientos que ayuden a cumplir las políticas; controles de acceso (físico y lógico) inadecuados, que permitan accesos no autorizados a ficheros o a datos transmitidos.”²⁷

Los entornos de procesamiento de la información son cada vez más sofisticados, a la vez que más distribuidos gracias a los avances en comunicaciones y redes; resultando a veces difícil poder garantizar razonablemente la seguridad de la información, y de forma especial su confidencialidad.

²⁷ Del Peso Navarro, Emilio y Miguel Ángel Ramos González **Confidencialidad y seguridad de la información: La LORTAD y sus implicaciones socioeconómicas**. Pág 79.



3.4. Protección de datos en la Internet, ley aplicable y estándares internacionales

“En el marco de la 31 Conferencia Internacional de Privacidad, se aprobaron los nuevos estándares internacionales de privacidad. Estos estándares definen un conjunto de principios y derechos encaminados a garantizar la efectiva protección de la privacidad a escala internacional; así como facilitar el flujo internacional de datos personales.

En los estándares se definen pautas especiales para la protección de la privacidad online: recomendaciones para redes sociales, buscadores online y plataformas web en general. A continuación un breve resumen sobre todo lo sucedido en Madrid.”²⁸

“En la 31 Conferencia Internacional de Privacidad se reunieron las autoridades de protección de datos de 50 países, así como numerosas instituciones y expertos de los campos de la empresa, la tecnología o la política de los cinco continentes; para analizar con detalle los retos a los que se enfrenta la privacidad y a los que tendrá que hacer frente en el futuro.

En el marco de esta conferencia, las autoridades de protección han adoptado una resolución que acoge favorablemente la propuesta conjunta de estándares internacionales de privacidad y la constatación de la necesidad de un marco global de privacidad y protección de datos. Los principios de lealtad, legalidad, proporcionalidad,

²⁸ Santos, Estefanía. **Un blog sobre internet y derecho**. <http://www.estefaniasantos.com.ar/areas-de-practica> (Guatemala, 29 de noviembre de 2013).

calidad, transparencia y responsabilidad que recoge el texto no sólo son comunes a los diferentes textos legales sino que cuentan con un amplio consenso en sus respectivos ámbitos geográficos, económicos o legales de aplicación.”²⁹

Entre las principales conclusiones debatidas en las principales sesiones destacan las siguientes:

3.4.1. Sociedad vigilada

“Expertos políticos coincidieron en que si bien es cierto que la seguridad y la libertad pública no son polos opuestos, el intercambio de información entre países es crucial en la lucha contra el terrorismo. En el marco del debate, los expertos destacaron que en una sociedad obsesionada con el riesgo, no es un esfuerzo sencillo que una sociedad sea protegida pero no vigilada, y efectuaron una serie de recomendaciones, como probar cualquier programa que afecte a la privacidad, utilizar sistemas de anonimización de datos, compensar al individuo afectado por el sistema, garantizar el más alto nivel de transparencia y actualizar la normativa nacional y multinacional con elementos sólidos y reales.”³⁰

²⁹http://www.privacyconference2009.org/media/notas_prensa/common/pdfs/061109_2_global_privacida_d_protección_datos.pdf (Guatemala, 15 de noviembre de 2013).

³⁰ Santos, Estefanía. **Ob. Cit.**



3.4.2. Privacidad en la Internet

“Mientras los representantes de la industria de internet afirman que en sus plataformas es el individuo quien determina el uso de sus datos, y defienden que el marco regulador no ponga fin a la innovación; otros expertos remarcaron que los derechos del interesado deben ser ampliados para que el usuario se encuentre en igualdad de condiciones respecto de la empresa. Asimismo, advirtieron que la pérdida de privacidad puede desencadenar la pérdida de otros derechos y apuntaron la necesidad de establecer un diálogo a nivel mundial sobre la privacidad para así adoptar una perspectiva global.”³¹

3.4.3. Menores y la Internet

“Los expertos destacaron que si bien las redes sociales ofrecen oportunidades de autoexpresión, también entrañan riesgos como el ciber acoso o el acoso sexual por parte de adultos, y consideraron que la divulgación de la información entre los menores es un elemento fundamental para tomar conciencia de los riesgos que puede entrañar el uso de forma incorrecta de internet. También se destacó la necesidad de que las redes sociales implementen de forma urgente sistemas de verificación de la edad efectivos.”³²

³¹ **Ibid.**

³² **Ibid.**

3.4.4. Prevención y reacción ante las quiebras de seguridad

“Los expertos debatieron si es posible prevenir las quiebras de seguridad y cómo hacerlo. En este sentido, coincidieron en que, en gran medida, éstas se deben a errores humanos y que la seguridad de los datos todavía no es lo suficientemente valorada. Se abogó por promulgar leyes apropiadas, educar a las empresas y aplicar de forma efectiva las leyes a los infractores para provocar con ellas un efecto disuasorio.”³³

3.4.5. Privacidad en el entorno laboral

“Representantes de diversos estamentos debatieron acerca del impacto de la utilización de las nuevas tecnologías como instrumento laboral, como la video vigilancia o el control de emails personales, y la consecuente colisión entre los derechos del empresario y los del empleado. Los ponentes recomendaron un enfoque preventivo y no represivo de las prácticas de control del empresario sobre el desempeño efectivo de trabajo por parte de los asalariados. Asimismo, sostuvieron que estas precauciones deben combinarse con campañas de sensibilización para que los trabajadores conozcan los derechos que les asisten.”³⁴

³³ **Ibid.**

³⁴ **Ibid.**

3.4.6. La privacidad ante las nuevas técnicas publicitarias

“Los expertos se reunieron para determinar las claves del nuevo escenario en el que sitúa a la sociedad este nuevo tipo de publicidad y todos convinieron en que la solución pasa por la necesidad de encontrar un nuevo equilibrio entre los intereses de la industria publicitaria, los intereses de los consumidores y la innovación. La soluciones propuestas no sólo atienden al establecimiento de un acuerdo de estos actores con las autoridades de protección de datos; sino muy especialmente, a la asunción de compromisos empresariales de autorregulación.”³⁵

3.4.7. Privacidad y responsabilidad empresarial

“Representantes del mundo empresarial y de la protección al consumidor coincidieron en señalar que las políticas de privacidad son un elemento de valor añadido para las empresas y debatieron acerca de la idoneidad de las actuales políticas de privacidad. En este sentido, señalaron la necesidad de cumplimiento de unos mínimos internacionales de protección de la privacidad que puedan combinarse con la ética corporativa de las diferentes empresas. Asimismo, se destacó la necesidad de que las administraciones públicas deben garantizar más recursos para las autoridades de protección de datos, e instaurar sistemas de sanción verdaderamente efectivos allí donde los establecidos no son suficientes.”³⁶

³⁵ **Ibid.**

³⁶ **Ibid.**

3.4.8. Periodismo ciudadano

“Los expertos abordaron el problema que puede suponer para los ciudadanos la permanencia en el índice de resultados de los buscadores; al apuntar que los medios no siempre han sido diligentes al rectificar informaciones por lo que, en el ámbito de internet, esto puede suponer una pena permanente que actualice mediante un solo click un hecho ocurrido hace años. Asimismo, se mostraron de acuerdo al apuntar que el respeto a la privacidad es parte sustancial del ejercicio informativo, pero también en que la intromisión en la privacidad es circunstancial a esa información.”³⁷

3.5. El derecho a la intimidad y la protección de datos personales

“El derecho a la intimidad abarca aquello que se considera más propio y oculto del ser humano, es decir la información que mantiene para sí mismo. Pero es ineludible que el contacto permanente del ser humano con sus semejantes al interior de la sociedad a la que pertenece, así como todos aquellos avances tecnológicos que han venido desarrollándose en la sociedad, han comenzado a transgredir aquellos ámbitos que forman parte de la intimidad del ser humano.”³⁸

La intimidad, marcada por un matiz individualista, es la facultad destinada a salvaguardar un determinado espacio con carácter exclusivo, y que consiste en un derecho del individuo a la soledad y a tener una esfera reservada en la cual

³⁷ **Ibid.**

³⁸ García González, Aristeo. **Protección de datos personales**. Pág. 748.



desenvolver su vida sin que la indiscreción ajena tenga acceso a ella.

La intimidad como una disciplina jurídica ha perdido su carácter exclusivo individual y privado, para sumar progresivamente una significación pública y colectiva, consecuencia del desarrollo tecnológico. La privacidad más que un mero sentido estático de defensa de la vida privada del conocimiento ajeno; tiene la función dinámica de controlar la circulación de informaciones relevantes para cada persona. Desde otro punto de vista, la privacidad no implica solamente la falta de información que una persona puede obtener de otra; sino más bien el control que se tiene sobre esa información personal.

Frente a la actual sociedad de información resulta insuficiente concebir a la intimidad como un derecho solamente garantista de defensa frente a cualquier invasión indebida de la esfera privada; sin contemplarla al mismo tiempo, como un derecho activo de control sobre el flujo de información que afecta a cada persona.

El derecho a la intimidad, consecuencia del desarrollo tecnológico y el creciente almacenamiento de información relativa a la persona, es necesario que sea reconocido así como también es necesario el establecer mecanismos de protección que puedan hacer frente al uso y manejo de los datos personales.

La protección de la intimidad frente a la informática no significa impedir el proceso electrónico de informaciones, necesarias en el funcionamiento de cualquier Estado

moderno, sino el aseguramiento de un uso democrático de la información.

En consecuencia, si un derecho a la intimidad ha sido viable; un tratamiento y almacenamiento tecnológico de datos personales también lo puede ser. Por ende, un derecho a la protección de los datos personales también debe implicar el reconocimiento de este último derecho como fundamental.

3.6. El derecho fundamental a la protección de datos personales

La relación que existe entre el derecho a la intimidad y el derecho a la protección de datos personales ya ha sido analizada por diversos sectores doctrinales, normativos y jurisprudenciales. En una primera aproximación, cabe señalar que los datos de toda persona deben ser objeto de protección, para que estos puedan ser tratados o elaborados y finalmente ser convertidos en información; y en consecuencia, sólo ser utilizados para los fines y por las personas autorizadas.

“Es necesario señalar que la protección de datos es aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular el derecho individual a la intimidad, respecto del procesamiento manual o automático de datos.”³⁹

Debido a las nuevas tecnologías se ha permitido tratar, elaborar y transmitir informaciones como los datos relativos a la persona; lo que en consecuencia ha

³⁹ *Ibid.* Pág. 761.



supuesto la aparición de nuevos derechos y libertades; o bien, el replanteamiento de su contenido y su función.

Ahora, habrá que replantear que en realidad el peligro para la privacidad de la persona no radica en que se acumule información sobre ella; sino en que pierda la capacidad de disposición sobre ella y respecto a quién y con qué objeto se transmite.

Así, la intimidad más que un estado de autoconfinamiento supone una determinada calidad de la relación con los otros. Por lo que se trata de una condición social de la persona, en que ésta puede tener legítimo derecho a no revelar a los demás determinados aspectos de sus relaciones con otras personas y que juzga deben permanecer en un plano privado. Dicha facultad de elección de la persona sobre la revelación o no de información que le concierne constituye el núcleo de la protección de datos personales.





CAPÍTULO IV

4. Exposición de datos personales

La seguridad de los datos es proteger estos de una revelación no autorizada, modificación o destrucción sea accidental o intencional. La seguridad de los datos es sencillamente la protección de los datos de las siguientes exposiciones básicas:

a) Revelación accidental. La revelación involuntaria de los datos, por ejemplo:

- Distribución de salida al usuario erróneo.
- Transmisión a la terminal errónea.
- Copias viejas de copias impresas utilizadas como desperdicios del personal.
- Datos presentados pero sin ser solicitados.

b) Modificación accidental. El cambio involuntario de datos, por ejemplo:

- Error en el cambio de posiciones.
- Mal funcionamiento en hardware.
- Mal funcionamiento en software.
- Duplicación.



c) Destrucción accidental. La ausencia involuntaria de datos, por ejemplo:

- Catástrofes naturales.
- Dejar caer un paquete de discos.
- Perder un mensaje.
- Esperar un periodo indefinido.

d) Revelación intencional. Actos deliberados de revelación de datos

- Retención por el personal y lectura cuidadosa de las copias impresas en carbón
- Vender información.
- Forzar un fichero de datos.
- Distribución de datos a personas no autorizadas.

e) Modificación intencional. Actos deliberados para cambiar los datos

- Rehacer un fichero.
- Añadir datos.
- Ocultar los datos.
- Suprimir los datos.



f) Destrucción intencional. Es el acto deliberado de suprimir los datos.

-Disturbios.

-Sabotajes.

-Robos.

La exposición a la que se encuentran sujetos los datos personales es amplia y peligrosa, tanto que el robo de datos se ha convertido en un gran negocio de compraventa que ya ha logrado lucrar grandemente en todo el mundo. Este nuevo negocio no regulado viola los derechos de las personas a su intimidad, así como otros derechos; pero sobre todo representa peligro para la sociedad por el mal uso que se puede hacer de ellos.

4.1. La comercialización informal de los datos personales

La comercialización de bases de datos es una rama del marketing que se enfoca en el trabajo con información de clientes potenciales o actuales. Con el desarrollo de las nuevas tecnologías y en especial internet, se ha facilitado el acceso y la utilización de la información personal en forma masiva.

En la actualidad, cualquier usuario tiene la posibilidad de adquirir alguna aplicación que permita copiar automáticamente las direcciones de mail que figuran en las páginas web a medida que se navega; y esta facilidad ha permitido el crecimiento de un mercado



negro de bases de datos.

Este fenómeno también es llamado mercado informal de base de datos. Una simple cadena de correo electrónico es una recopilación y validación de direcciones de correo electrónico. Si se reenvía una cadena de correos electrónicos a varios amigos, se está validando el correo electrónico y contribuyendo a una base de datos.

Una fuente de información importante con la que cuentan las empresas para la recolección de datos personales a través de internet son los registros de compras. Las páginas web de compra y venta tienen abundante información, que luego se utiliza con fines estadísticos o para acciones de marketing. Las redes sociales, en especial las más populares como facebook, constituyen otra fuente a tener en cuenta, debido a que allí los usuarios dejan abundantes indicios acerca de sus intereses y hábitos, a medida que crean y participan en grupos temáticos y páginas de fans.

Un mayor uso de las redes sociales permitió que las compañías puedan generar sus propias bases de datos con el comportamiento de sus usuarios. Una empresa puede construir una base de datos a través de sus clientes, o se puede generar en forma espontánea, alrededor de una red social; como el fanatismo por determinada banda de música, determinado lugar o determinada marca. Se genera un grupo, que luego es aprovechado por alguien: por un líder de grupo, una empresa o alguien que quiere comunicar algo.



La piratería en páginas web de intercambio de archivos ha puesto de manifiesto que una de las fuentes de ingresos más importantes de estas páginas procedía de la venta de datos de usuarios registrados. La mayoría de estas webs exigen al usuario ceder sus datos para poder descargar películas o videojuegos. Este hecho es alarmante porque una gran parte de los usuarios que accede a este tipo de páginas es menor de edad.

Estas páginas no tienen ningún control sobre el tipo de usuario que se registra en ellas. Se puede registrar con datos falsos, pero lo que si piden es una cuenta de correo electrónico que esté activa, a la que después puede llegar publicidad pornográfica.

“A cambio de una contraprestación económica, las agencias de publicidad recibían de parte de los webmasters todos los datos recolectados de los registros de usuarios en estos portales. A través de esta forma de ingresos uno de los administradores logró percibir 145.000 euros aproximadamente.

Hábitos de consumo de video realizado por jóvenes menores de 24 años, son el blanco más fácil para descargar contenidos de este tipo de webs. Por otro lado, una de las compañías más importantes de e-mail marketing refleja en su informe de auditoría que el 36% de los suscriptores de páginas web son menores de 24 años, de los cuales el 24% es menor de 18 años.”⁴⁰

⁴⁰ <http://www.noticiasdot.com/wp2/2007/05/15/la-venta-de-datos-personales-de-usuarios-es-la-mayor-fuente-de-ingresos-de-los-portales/> (Guatemala, 12 de noviembre de 2013).



De igual forma, cualquier persona puede tener en su poder los números telefónicos y direcciones de clientes e información de personas con altos ingresos que se pueden descargar de la web al hacer una transferencia bancaria.

En el caso de Guatemala, las empresas están ofreciendo, por medio de correos electrónicos, las bases de datos de más de 11 millones de guatemaltecos que contienen los nombres completos, números telefónicos, domicilio completo y el límite de crédito según sus ingresos.

4.2. Consecuencias de la revelación de datos personales

Una de las consecuencias que trae la revelación de datos personales o la compra ilegal de los mismos es que caiga en las manos equivocadas; es decir, que los fines con los que se obtengan lleven consigo la voluntad de dañar a las personas cuyos datos fueron revelados; esta consecuencia a corto plazo puede llegar a afectar la integridad física de las personas; es decir, se pone en riesgo su seguridad tanto física, económica como moral. En este plano los cuerpos de seguridad tanto como empresarios por mencionar algunos; son los blancos más populares, ya que los primeros pueden ser grandes enemigos de los delincuentes y los segundos pueden parecer a los delincuentes una fuente de ingresos para secuestrarlos, robarles o incluso amenazarlos de muerte.

La revelación de datos personales también conlleva daño a la reputación de las personas o su dignidad dependiendo que tipo de datos sean los revelados; por ejemplo



su religión, orientación sexual o preferencia política. Además de dañar su reputación y su dignidad, en muchas ocasiones esos mismos factores pueden perjudicar sus relaciones laborales y sociales.

4.3. Análisis jurídico de la protección de datos personales y su comercialización

Para regular la comercialización de datos personales es necesario establecer límites, tales como los indicados a continuación.

Primero, es necesario definir qué comprenden los datos personales en una definición muy amplia pero útil; para así poder encuadrar dentro de la misma cualquier supuesto de tratamiento que surja como consecuencia del avance de las tecnologías.

El ámbito de la protección debe ser aplicable a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento; así como a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Estos parámetros ciertamente protegerán los derechos fundamentales y las libertades públicas y en particular el derecho a la intimidad y el honor de las personas físicas. Los principios de la protección de datos que deben de tomarse en cuenta son:



- Calidad de los datos

Los datos de carácter personal sólo se podrán recabar para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos; en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Estos condicionantes han de ponerse en relación con el caso en concreto.

- Finalidad

Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquéllas para las que los datos se hubieran recolectado. No se considerará incompatible el tratamiento posterior de estos con fines históricos, estadísticos o científicos.

Los datos de carácter personal incorporados al fichero han de responder a la situación actual; de manera que recojan todas las modificaciones surgidas y una vez incorporadas responderán a la realidad.

Asimismo, los datos de carácter personal han de ser exactos, de manera que si resultan ser inexactos o incompletos, en todo o en parte, han de ser cancelados o sustituidos de oficio por el responsable del fichero.

Cuando se ha cumplido la finalidad para la que se recabaron los datos, han de ser cancelados o destruidos, en caso de no ser posible han de ser bloqueados.

No serán conservados en forma que permitan la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Se prohíbe la obtención de datos por medios fraudulentos, desleales o ilícitos.

- Información

Los interesados a los que se les soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

- a) De que sus datos van a ser incluidos en un fichero, de la finalidad de la recogida y de los destinatarios de la información.
- b) De la obligatoriedad o no de dar esos datos.
- c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- d) De la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.



e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante para que los afectados puedan ejercer sus derechos.

Todas estas advertencias deberán constar en aquellos cuestionarios e impresos utilizados para la recogida de los datos.

- Consentimiento

El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco; es decir, expreso o tácito del afectado, para los datos especialmente protegidos consentimiento expreso y por escrito dada la importancia de los mismos.

- Seguridad de los datos

El responsable del fichero deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

El responsable del fichero es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio o



cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

- Deber de secreto

Tanto el responsable del fichero como el encargado del tratamiento, así como cualquier persona que intervenga en cualquier fase del proceso, están obligados al secreto profesional respecto de los mismos y al deber de guardarlos; obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

- Derecho de acceso

El interesado tendrá derecho a solicitar por escrito, ya que si no queda constancia se entiende que no se ha realizado; a obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

- Derecho de cancelación

Es el derecho que tienen los afectados a cancelar los datos de carácter personal recogidos en los ficheros. El responsable del tratamiento tendrá la obligación de hacer efectivo este derecho, y en caso de que dicha cancelación no sea posible se procederá



a su bloqueo.

- Derecho de rectificación

Los ficheros deben cumplir con el principio de calidad, por ello es posible ejercitar este derecho con el fin sustituir los datos erróneos por los válidos.



CONCLUSIONES

1. La regulación normativa de la protección de datos personales en el comercio electrónico guatemalteco se encuentra en un atraso momentáneo; como consecuencia de la magnitud y evolución que lleva a cabo el desarrollo del comercio electrónico.
2. Guatemala no cuenta con una legislación apropiada de protección de datos personales en el comercio electrónico, únicamente cuenta con la Ley de Información Pública que regula a las entidades del Estado y demás reguladas en la misma; dejando a un lado al resto de personas individuales o jurídicas que pudieran aprovechar la captación de información para su comercialización.
3. La legislación carece de mecanismos jurídicos válidos que protejan la comercialización de datos personales en el ámbito privado, ni se ha discutido el tema con amplia participación; dejando así un vacío legal y una laguna para la comercialización de datos personales.
4. La comercialización de datos personales carece de protección institucionalizada, como consecuencia su actividad dentro del comercio electrónico ha proliferado; creando así una red de datos sensibles personales que pueden afectar tanto la dignidad como la intimidad personal.



5. Uno de los aspectos positivos de la participación de las naciones a nivel mundial en el asunto protección de datos y la comercialización electrónica, resulta ser la participación de la Organización Mundial de la Propiedad Intelectual, delegación de la Comisión Europea en donde se presenta la protección sui generis de bases de datos.



RECOMENDACIONES

1. En base a lo preceptuado en la Constitución Política de la República de Guatemala, el Estado de Guatemala, debe procurar la creación de leyes específicas encaminadas a la protección de los datos personales de los ciudadanos.
2. Que el Organismo Legislativo presente iniciativas de ley para la protección de los datos personales, así como para la organización y control de la comunicación en el correo electrónico.
3. Establecer políticas de gobierno electrónico que permitan la protección de información, creando instituciones que velen por la seguridad jurídica en el ámbito informático y delimiten el accionar de la misma en el mundo material con facultades sancionatorias.
4. Establecer y crear protección institucionalizada, para la protección de datos personales y así evitar la comercialización de los mismos en el comercio electrónico, garantizando y protegiendo la dignidad como también la intimidad personal de las personas que puedan estar vulnerables a dichos actos.



5. Que en adelante, se intensifiquen las convenciones y tratados internacionales relacionados con los avances de la tecnología; elaborándose un análisis jurídico en cuanto a la necesidad de velar por la protección de los datos personales y fortaleciéndose las leyes ya existentes que regulan dicho aspecto legal.



BIBLIOGRAFÍA

- ARGÜELLO, F. **Protección de datos personales: la directiva comunitaria, su influencia y repercusiones en Latinoamérica. II Encuentro Iberoamericano de Protección de Datos.** La Antigua- Guatemala, 2-6 de junio de 2003. Valencia, España: Ed. Tirant lo Blanch, 2005.
- BARRERA LÓPEZ, Horacio Mauricio. **El derecho informático en la currícula universitaria.** Guatemala: Ed. Sir Speedy, 2007.
- BRUCE, O. **Comercio electrónico y derechos del consumidor. Revista de Ciencias Jurídicas.** No. 99. Setiembre-Diciembre 2002. Costa Rica: Ed. Colegio de Abogados, Facultad de Derecho de la Universidad de Costa Rica, 2002.
- CABANELLAS, Guillermo. **Diccionario jurídico elemental.** 18va. ed. Buenos Aires, Argentina: Ed. Heliasta, 2006.
- CAMPOS, Celin. **La propiedad intelectual y el Decreto 165/94.** Tucumán, Argentina: Ed. Revista Jurídica Número 29 de la Facultad de Derecho de la Universidad Nacional de Tucumán, 1997.
- CHEN SUI, Susan. **Déficit y oportunidades de la legislación costarricense sobre comercio electrónico.** San José, Costa Rica: (s.e.), 2008.
- CHIRINO, A y M. Carvajal. **El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica.** Revista Costarricense de Derecho Constitucional. Tomo IV. Costa Rica: Ed. Investigaciones Jurídicas S.A., 2003.
- DEL PESO NAVARRO, Emilio y Miguel Ángel Ramos González. **Confidencialidad y seguridad de la información: La LORTAD y sus implicaciones socioeconómicas.** Madrid, España: Ed. Díaz de Santos, S.A., 1994.
- Dirección Nacional del Derecho de Autor. **Génesis y evolución del derecho de autor.** 2da ed. Bogotá, Colombia: (s.e.), 1995.



GARCÍA GONZÁLEZ, Aristeo. **Protección de datos personales**. México: Ed.IUS UNLA, 2011.

HEREDIA QUECAN, César. **La protección jurídica a las bases de datos**. Colombia: (s.e.), 2002.

<http://www.noticiasdot.com/wp2/2007/05/15/la-venta-de-datos-personales-de-usuarios-es-la-mayor-fuente-de-ingresos-de-los-portales/>. (Guatemala, 12 de noviembre de 2013)

http://www.privacyconference2009.org/media/notas_prensa/common/pdfs/061109_2_global_privacidadproteccion_datos.pdf. (Guatemala, 15 de noviembre de 2013)

MENÉNDEZ, J.C. **El contrato vía internet**. Barcelona, España: Ed. J.M. Bosch Editor, 2005.

Organización Mundial de la Propiedad Intelectual. **Documento CRNR/DC/6**, Ginebra, Suiza: (s.e.), 1996.

Organización Mundial de la Propiedad Intelectual. **Documento CRNR/DC/100**, Ginebra, Suiza: (s.e.), (s.f.).

OSSORIO, Manuel. **Diccionario de ciencias jurídicas, políticas y sociales**. 26a. ed. Buenos Aires, Argentina: Ed. Heliasta S.R.L., 1999.

PEÑA ORTIZ, Paola y Catalina Achío Gutierrez. **El derecho al olvido**. San José, Costa Rica: (s.e.), 2011.

PIERINI, Alicia. **Hábeas data, derecho a la intimidad**. Buenos Aires, Argentina: Ed. Universitaria, 1998.

PINOCHET, R. **Contratos electrónicos y defensa del consumidor**. Madrid, España: Ed. Marcial Pons Ediciones Jurídicas y Sociales S.A., 2001.



PINOCHET, R. **Contratos electrónicos y defensa del consumidor**. Madrid, España: Ed. Marcial Pons Ediciones Jurídicas y Sociales S.A., 2001.

PUIG PEÑA, Federico. **Compendio de derecho civil español**. Pamplona, España: Ed. Aranzadi, 1979.

SANTOS, Estefanía. **Un blog sobre internet y derecho**.
<http://www.estefaniasantos.com.ar/areas-de-practica> (Guatemala, 29 de noviembre de 2013)

SARRA, A.V. **Comercio electrónico y derecho: aspectos jurídicos de los negocios en internet**. 1. ed. Buenos Aires, Argentina: Ed. Astrea, 2000.

TELLEZ VALDEZ, Julio. **Derecho informático**. 2da ed. México: Ed. McGraw-Hill, 1996.

Legislación:

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

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

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

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

Ley de Acceso a la Información Pública. Congreso de la República de Guatemala Decreto número 57-2008,2008.